Guide to: Hacking, Carding Phreaking By: The Dark Lord

Introduction:
~~~~~~~~~~~~~~

This is a text file is Made By The Mickey Mouse Club and would ask that it would be distibuted to others for there use. This file is going to go into depth on how to Hack, Phreak, and card. There will be information that should help everyone, Hopefully!!

Hacking:
~~~~~~~~~~

Hacking is a long hard process, unless you get lucky. There are many programs and aids out to make the job a lot easier, but the concept is the same no matter how you use it. First, at least on most things that you hack, you need to get some type of account or vacancy, etc... This is done by randomly entering numbers and or letters until you come up with the proper combination to find the account. Knowing the size of the account number makes this job one-hundred times easier. Thats why I suggest you find out from someone who allready has one or card one. By carding the account, it will die quickly but at least it will give you the length of the account numbers (More on that topic will be expained in the carding section). The accound numbers, do not always just contain numbers or have numbers at all in it. If it has a mix, it makes it a hell of a lot harder to get. You will just have to experiment to find out what charactors are contained in the account. Some Examples of ones that do have mixes of numbers and letters would be Pc Persuit accounts. The forms of them are usuall as such:

Account: Pgp014764g
Password: 23632k

It looks from these that you are pretty much screw because of the way letters are mixed with numbers, thats what makes having a program so much easier. In a lot of circumstances, getting the account is the hardest part that is why having a good background of the system is a major plus in your favor. Once you have got the account, it is time to get the password for this account. Once again having the length and such makes this process not only easier, but faster. just keep entering random passwords of the length or the thought length in until you get a stoke of luck and get it. You MUST remember that 99.5 out of 100 times, this is a long process, and you have to have patience. If you don't you might as well forget ever getting on to the system or have someone else do it for you. Once you have gotten the password, look it over long and hard. Write it down and keep it, examine it. 99% of the time there is a pattern to all the account passwords. Things to look at is the password in reference to the account number. check to see if things have been added to the end or beginning like 00 or 01 or 99 of 0010 thing like that. If you see no relations,

the only other way to really find out the pattern in to get another one. Look at both of them together, see if there the same or it account 400's password is 3456 and 402's password is 3458 (they go in order) then just those as a reference to other passwords, take away so much from accounts with a lower number and add the required amounts to accounts with a higher number, etc.... But bassicly, LOOK FOR A PATTERN! Once you have got the password and the account, you have got yourself a passage way in.

Although this is what you do to succeed, you have to take many precautions. They do NOT like us messing with the system and they obviously want you to pay just like the others, so they will take necessary means to nail you. They trace like you wouldn't belive. They will trace right as you get on, if you happen to be unlucky,

you will never know when they are doing it either, you must ALWAYS be aware of the dangers and take precautions! Even on things that you wouldn't think that they would trace you but, be carfull. Whether they trace depends on a couple of things, here are a few major ones:

1. There bank balance
2. There desire to catch you
3. The amount of infestation in there system

There are things that you can do to protect yourself, these are not all of them and none of them are sure fire ways, but hey, cutting down your chances of getting caught makes a world of difference, because remember, All the fun is taken away if you caught. Some things to do to protect yourself is:

1. Use a diverter
2. Use false information about you
3. Never stay On-line too long
4. Call during late or early hours, were there is most likely no one monitoring the system
5. Don't call frequently or during the same hours, regulate it

Once again these are not all of them but these are some of the "More" helpfull things. If you follow all the step, you can reduce the change of getting caught by about 40%. f you do get caught there is not a whole lot that you can do, but some tips are, first, don't reveal any information on what you have done. Deny all charges. Sencond, plea bargin with knowladge of things, like hacked sytems etc.. But never admit that you did it. Three, and most important, get a GOOD LAWYER!!!!!!!

DIFFERENT TYPES OF SYSTEMS:

Pc Persuit Cp\m, Trw, Unix, Vmb, Vms

These are just a few systems, if I made a complete list There would be pratically no end to it, there are millions.

Phreaking:
~~~~~~~~~~
Phreaking, Ahhhwwww, the wonderfull world of phreaking. Well to start with Phreaking is "The use of Telecommunications to others besides people of the Phone Company". Well thats my version of the definition at least. Using codes is wuit easy, there are different parts to it, the Dial-up, the code, and the number. First you will have to dial in the dial-up and on most dial ups you will get a tone or a buzz or click or something to that effect. Once you hear this, and you will know when you hear it you dial in the code. Sometime you will get another tone or beep etc. and when you do that is when you dial in the number. If you do not get another tone or whatever you just dial in the number right after you enter the code. You might have to have a test dial up to see how the tones go. In dialing the number once agian the nubers differ. You must enter the area code and then the nuber. Some require that you have a one before the area code but most that I have used do not. You can tell if the code worked right after the number has been put in not just by the error recording that you get but if right off the bat the phone begins to ring, it doesn't work. A code can also be busy. If it is busy it could mean that the code is dead or that too many people are using it at once. You might experiance this often. There are numbers that make phreaking much safer, they are called diverters. What the do is when the number that you have dial is being traced it diverts it to that number. Unless this is virgin or nobody else uses it, you will find that with in a couple of days after it is out, it
~~~~~~~~~~

will be busy, that is the annoyance about diverters, and they are also hard to get. Hacking is also put into play in phreaking by using programs to get dial ups and the codes. Getting these are done in the same way you hack anything else. Just get a program like code thief or code hacker, or make one yourself, it is quite easy. There is a danger with useing the codes. If you hack a code yourself, not just the code but the dial up amd no one else has it you can pretty well bet that it is safe. A newly hacked dial-up/code is considered "Virgin". those Ma bell is not having the problem with people phreaking off of it so they don't bother doing anything with it. But after a while, it will either Die (No Longer work) or they will start tracing off of it. The whole pain about it is, is you will never positively no when they started doing traces or things like that. The codes might be being traced but you are getting the luck of the draw. On most codes they don't trace on every call, they just file it away and watch for like the 50th or 100th caller and then that person gets nailed. You might think if they do trace every 100 calls, that means you have a 1 in 100 chance of getting caught and those are really good odds. Well the odd is 100 to 1 but the is a lot of people that live in areas that they can call with that code. If you figure about 10 million people could use it then about 100,000

of them are. 100,000, hummmmmmm, how odes your odds look now. In a couple minute time spand 99 peoplecould have used it, and lucky you might be the 100th caller. A lot of times the take like every hundered calls and then when they get the 100th caller, that don't just trace one, they trace 100, 101, 102, 103, 104 200, 201, 202 etc. So you chances of getting caught when the heat is on the code is pretty good. There are a couple different types of codes and the two major ones are 1-800's and 950's. 800's can pretty much be dialed from anywhere in the states, but 950's stay in certain areas. Some 950 dial ups are:

9501001
9500266
9500355
9501388

And there are others, but like take me for example, where I live you cannot use 9500266. It will tell you that you cannot use that number from your dialing range or it just won't work. You might get to the point where the dial-up works but not the code. If this is the case it will say: "Invalid authorization Code" Some examples of 1-800's are as follows:

1-800-255-2255
1-800-759-2345
1-800-959-8255

There are many others but those are just a few, very few. There are also 1-800's and others that will send you directly to the operator, you must tell her the code and the number you are dialing. These are NEVER safe to use. but in one case they are alot better. I am out of town a lot so I have to use pay phones right? Well, you are safe with anything with pay phones, so that is a good way to call people. The real good thing them though, is since you must go throught th operator, the codes stay valid for up to 10 times as long as the others. But thenm again another draw back is it is not a line that you want to give real names or numbers over. Because these are often tapped, since the operator know that you used the code, they will listen in quite often, and you will never even notice. Another problem experianced with them is if you are what MMC calls

"Petite Flowers", our home made word for , someone that sounds like a little kid, then they really give you a hastle about using the code. I have had a lot of people ask me if the person you are

calling with the codes can get busted. The answer is "No". They cannot do anything to the person, just ask him who is calling him with the codes, and they rarely do that. Just let the person you are talking to, if they don't already know, not to tell anyone that you are calling with the codes. The phone companies do have to option of setting up a trace on that persons line and bust you when you do call

him with a code. I have never seen this done but do be aware that the phone companies are made up of intellegent adults and they are very smart and can and will nail you in many ways. I am a firm beliver that you should share a the information that you other phreakers and hackers as they should do the same with you. I also see an execption, inexperianced people. They can run it for everyone be not have the knowladge and screwing up. I realize that they need someway to build themselves up to a good phreaker but be cautions in what you give to them. Codes die really often and you really have to keep up with the phone company. Its kinda of a pain to keep up with it on your own as quickly as they work but thats why there is phreaking communities and groups such as Fhp and MMC, the gives the edge to the phreakers in the way that, you have help in keeping up with the phone companies, and in most cases if the groups or communities are working well together, you can eve stay one step ahead of good 'ole Ma bell and others. You really need to find ways of getting codes either from getting acess to the phreaking sections on the pirate boards you call or throught friends, Vmb's Loops, Confrences, etc., just try to find a good connection to people that are into phreaking too.

Carding:
~~~~~~~~~

Although everything talked about in the text file to this point is illegal, and you will get busted if you get caught, this is one one the one that you can get in some major shit over. About the only thing I have talked about that this falls short of is hacking a government compter, and thats one of the Grand daddies of them all. Well, although it is a major crime, it is really cool!!!! This is the process in which you find the card number of someone and use it to purchase things. In order to card, there are a few things that you must have or it will not work. You will need to have.....

1. The Card Number
2. The Experation date
3. Card type (Master Card, Visa, etc...)

Those are the main things tha you will need. Having the name of the owner is very helpfull but it is not a must. You can get by without it. You have to order everything you want by mail. A couple of "Beginner" carder that I talked to didn't understand how you would do it, but thats when they had the misconception that you actually go to the store and purchase things. That is a complete No, no. You do everything from a phone ordering service. When you call make sure that you are a t a pay phone. Don't do it your house or anywhere where it can come back to you. When you order the merchandice, once again do send it to anywhere that it can come back to you like your home, work, etc. Find a vacant house or building or anywhere else that you can send it to. Also, don't send it to a P.O. box that you have, just as dangerous.

When you do order it and you think its around the time that you will be reciving it, check the mailbox frequently. But do it during odd hours. I mean, hows it going to look you taking a package from a vacant house? Most bills are sent at the end of the month or at the biginning, so try to time it to where the bill won't come to the person untill a couple of days after you have
~~~~~~~~~

recived the package. Ok heres how to figure it. I have found out that the bills are sent out up around the 26-30th of the month, so they will actually recive the bill around the 31-4th. Have it sent right after you think the bill has been sent. Find what you want, but try to order it from the place that guarentees the fastest delivery. When you order the item, make sure they have it in stock and don't have to get the item in first. Order the highest class of delivery but not COD or next day service. Thats cutting it too close. It should take around 2-4 weeks before you get it and if you timed it right, then it sound get there right before the person gets the bill. You need to have it in your possesion before the bill gets to the person because if they complain, they can keep it from being sent, or watch who actually gets it even while its going throught the mail process. Don't order more than a couple of things or overcharge the card, if the people at the Credit card office, see irregular charging on the card, they will follow up on it. To actually order the item you will call up the place that you will be ordering from, and when the operator answers let her know what you need to as far as what you are purchasing, etc. When she ask how you will be paying just tell her "Charge" and the the type of card like Master Card, Visa, ect. Then Tell them your name, if you don't know the name of the actuall owner of the card, Make up a false name that has NO relation to your name, not the same first, last middle what ever, nothing relating to your real name. Then continue answering all the operators questions, address (Not your own remember!) state, area code etc. They will also ask for your phone number. Make one up, not your own. If something happens to go wrong as far as delivery or if they are checking if you are who you say, then your screwed, unless of course, hehehe, the number is ALWAYS busy. Find the busiest number there is and leave them that. When they ask for the card number and experation, just tell them and do what all else you need. Wish them a good day, and hope you get it. Ok heres how you check if the card is good, and how much money can be charged on the card.....

1. Dail 1-800-554-2265
2. it will ask for the type of the card. you must put in 10 for Master Card and 20 for Visa, I am not sure about the others.
3. Next it will ask for the Identification. You will need to enter 1067
4. After all that you will have to enter the Mecrchant number, which you will either need to put in 24 or 52. One of them should work.

5. You will then have to enter (When Prompted) the card number itself.
6. Next, the experation date of the card.
7. Last but not least the amount you want to try to get on the card. The procedure for this is enter dollars, astricks, then cents. (Example:) 100*30 = One hundred dollars and thirty cents. One thing I do need to mention, after you type in everything you must press pound (#). Like when it asks you for the type of card, if you had a Master Card you would put: 10#. when it asked for identification you would enter 1067#. If it says invalid, that either means that the card is no good or you can't charge that amount on the card. Try it again, but try a lower amount. If you get down to $1 and it still doesn't work, hehehe, you can probably guess that the card is no good. You might not be ordering just merchandice you might be ordering accounts and things like that and if you are, fine, but you have to remember, the accounts do not stay good for very long, the owner of the card gets the bill, complains and its no longer any good. And when you card and account, Nine out of ten times, they won't kill the account, they will trace in and that is when you butts really in a sling. So carding accounts and things, isn't the safest way to go, of course. nothing we have talked about it, right?

Conclusion:

~~~~~~~~~~~~~~

Well thats about it for now, there should be a BIG newsletter by The mickey Mouse Club comming out soon that you have to be sure NOT to miss. I sincerely hope that you have gotten alot out of this newsletter and I would like to ask for suggestions and Ideas to make MMC a better orginazation. At this time myself and Cardiac Arresst have a Vmb at: 1-800-444-7207 [Ext] 4001. All ideas and suggestions, please bring there. Also, since your making the trip anyways, bring along some phreaking codes and all and any types of accounts. I would be greatly appreciated by: The Mickey Mouse Club.

LOD/H BUST By Pizza Man

" U.S. computer investigation targets Austinites "

[The above caption high-lighted the Saturday March 17, 1990 edition of the Austin American-Statesman [Austin, Texas]. The article has been copied in its entirety, and the main point for typing this up was because of the involvement of the LOD/H throughout the article.]

The U.S. Secret Service has seized computer equipment from two Austin homes and a local business in the past month as part of a federal investigation into electronic tampering with the nation's 911 emergency network. Armed Secret Service agents, accompanied by officers from the Austin Police Department, took the equipment in three March 1 raids that sources say are linked to a nationwide federal inquiry coordinated by the Secret Service and the U.S. attorney's office in Chicago. While federal officials have declined to comment on the investigation - which focuses on a bizarre mix of science fiction and allegations of high-tech thievery - the Austin American-Statesman has learned that the raids targeted Steve Jackson Games, a South Austin publisher of role-playing games, and the home of Loyd Blankenship, managing editor at the company. A second Austin home, whose resident was acquainted with Jackson officials, also was raided. Jackson said there is no reason for the company to be investigated Steve Jackson Games is a book and game publisher of fiction, he said, and it is not involved in any computer-related thefts. The agents, executing search warrants now sealed by a judge from public view, took computer equipment, including modems, printers, and monitors, as well as manuals, instruction books and other documents. The equipment has been forwarded to federal officials in Chicago. The Secret Service, best-known for protecting the president, has jurisdiction in the case, government officials say, because damage to the nation's telephone system could harm the public's welfare. In addition, the system is run by American Telephone & Telegraph Co., a company involved in the nation's defense. The 911 investigation already has resulted in the indictment of two computer "hackers" in Illinois and sources say federal authorities now are focusing
~~~~~~~~~~~~~~

on Austin's ties to a shadowy underground computer user's group known as the Legion of Doom.

The hackers, who live in Georgia and Missouri, where indicted in Chicago. they are believed to be members of the Legion of Doom and are charged with seven counts, including interstate transportation of stolen property, wire fraud, and violations of the Computer Fraud and Abuse Act of 1986.

The government alleges that the defendants stole a computerized copy of Bell South's system that controls 911 emergency calls in nine states. The information was then transferred to a computer

bulletin board and published in a hacker publication known as Phrack! A trial in the case is scheduled to begin in June. U.S. agents also have seized the final drafts of a science fiction game written by the Austin-based game company. Sources say the agents are trying to determine whether the game - a dark, futuristic account of a world where technology has gone awry - is being used as a handbook for computer crime. Steve Jackson, the owner of the local company and a well-known figure in the role-playing game industry, said neither he nor his company has been involved in tampering with the 911 system.

No one in Austin has been indicted or arrested as a result of the investigation. "It is an on-going investigation. That is all I can say," said Steve Beauchamp, special agent-in-charge of the Secret Service Austin field office. "Until we can put it all together, we just do not comment," he said.

Bob Rogers, Jackson's Dallas attorney, said federal officials have assured him that neither Jackson nor Jackson Games is the target of the probe. The authorities would not tell Rogers whether the inquiry focused on other company employees. As for the science fiction game, called Cyberpunk, Jackson said federal authorities have mistaken a fictional work for a technical manual [E.N. Why does this sound all too familiar?] . "It's not a manual for computer crime any more than a Reader's Digest story on how to burglar-proof your house is a manual for burglars," said Jackson, 36. "It's kind of like the hints you get on safe-cracking from a James Bond movie."

Blankenship, the author of the book, said his attorney has advised him not to comment on the book or the Secret Service investigation. Jackson said he guesses his company was linked to the 911 probe by its use of a computer bulletin board system, called Usenet. The board, one of hundreds throughout the country, is a sort of electronic Town Square, where personal computer users from throughout the world can tap into the system via phone lines and a modem.

The network, free and relatively unregulated, is an information exchange where users can post information, exchange electronic messages and debate with keyboards everything from poetry and politics to nuclear war. One of the world's largest networks - boasting more than 600,000 users - Usenet was tapped by Chinese students in North America to organize support for students during the pro-democracy demonstrations last year. The network also was infected in 1988 by a now-famous computer "virus" unleashed by college student Robert Morris. Jackson said his company has maintained a bulletin board on the Usenet network on which it posts advanced copies of its role-playing games. The firm posts the games and requests that the users of the network comment on the text and propose improvements. The Jackson bulletin board, called Illuminati, greets users with the

company's logo and a message that states: "Welcome to the World's Oldest and Largest Secret Conspiracy." Over the past several months, the company has been posting drafts of Cyberpunk for review. The resident of the second Austin home raided by the Secret Service was acquainted with Jackson and had made comments about the game on Usenet. He asked to remain anonymous. Typical of Cyberpunk literature, the game is set in a bleak future, much like the world portrayed in Max Headroom, formerly a network television program. Computers and technology control people's thoughts and actions and are viewed both as a means of oppression and as a method of escape. Portions of Jackson's Cyberpunk viewed by the Austin American Statesman include a detailed discussion on penetrating government computer networks and a list of fictitious programs used to break into closed networks. Bruce Sterling, an Austin science fiction writer and one of the world's best-known Cyberpunk writers, said Jackson's game and its computer-related discussions are hardly unusual for the genre. "Cyberpunk is thriller fiction." Sterling said. "It deals to a great extent with the romance of crime in the same way that mysteries or techno-thrillers do." He said the detailed technical discussions in the Jackson games are what draws people to them. "That's the charm of simulating something that's supposed to be accurate. If it's cooked up out of thin air, the people who play these games are going to lose interest."

Jackson, though, said he has been told by Secret Service agents that they view the game as a user's guide to computer mischief. He said they made the comments where he went to the agency's Austin office in an unsuccessful attempt to reclaim some of his seized equipment. "As they were reading over it, they kept making outraged comments," Jackson said. "When they read it, they became very, very upset. "I said, 'This is science fiction.' They said, 'No. This is real.'" The text of the Cyberpunk games, as well as other computer equipment taken from Jackson's office, still has not been returned. The company now is working to rewrite portions of the book and is hoping to have it printed next month. In addition to reviewing Cyberpunk, sources say federal authorities currently are investigating any links between local computer hackers and the Legion of Doom. The sources say some of the 911 information that is the subject of Chicago indictments has been traced to Austin computers. Jackson's attorney said federal officials have told him that the 911 information pilfered from Bell South has surfaced on a computer bulletin board used at Steve Jackson games. But the information apparently has not been traced to a user. Jackson said that neither he nor any of his employees is a member of the Legion of Doom. Blankenship, however, did consult with the group in the course of researching the writing the Cyberpunk game, Jackson said. Further, the group is listed in the game's acknowledgments for its aid in providing technical information used in Cyberpunk. For these reasons he believes Blankenship is

a local target of the federal probe, though none of the investigators has yet confirmed his suspicion. "My opinion is that he is (being investigated)," Jackson said, "If that's the case, that's gross. he had been doing research for what he hoped would be a mass-market book on the computer underground," Jackson said. The other Austin resident raided by the authorities, who asked to remain anonymous, acknowledged that he is the founding member of the Legion of Doom and that copies of the 911 system had surfaced on the group's local bulletin board. The 20-year-old college student said the information hardly posed any threat to the 911 system. "It was nothing," he said. "It was garbage, and it was boring." In the Chicago indictment accuses the group of a litany of electronic abuses, including: disrupting telephone service by changing the routing of telephone calls; stealing and modifying

individual credit histories; stealing money and property from companies by altering computer information; and disseminating information about attacking computers to other computer hackers. The Austin Legion of Doom member said his group's worst crime is snooping through other people's computers. "For the most part, that's all we do," he said. "No one's out ripping off people's credit cards. No one's out to make any money. "We're just out to have fun." The group member said the fact that the legion is shrouded in mystery adds to its mystique - and to the interest law enforcement agents have in cracking the ring. "It's an entirely different world," the student said. "It's a very strange little counter-culture. "Everybody who exists in that world is familiar with the Legion of Doom," he said. "Most people are in awe or are intimidated by it."

A shadowy gang of computer hackers with ties to Austin has become the target of a massive federal probe into the nation's high-tech underground. Federal and local authorities involved in the inquiry seized evidence from three Austin homes and a business in March. They say some action on the local cases, possibly including indictments or arrests, is expected in the next month.

The computer crime crackdown - the largest ever launched by the U.S. government - has resulted in the temporary disbanding of the Legion of Doom, a notorious national group of young computer hobbyists with at least two Austin members. State and federal investigators say the 6-year-old group, which once boasted more than 150 members in nearly every U.S. state, has been connected to a string of computer crimes in Texas, Georgia, Arizona, Illinois, California and New Jersey. Officials say group members have electronically stolen money and long-distance telephone access numbers, changed credit reports, planted datadestroying computer viruses in government networks, attempted to tamper with hospital patient records, and distributed information that, if used, could have debilitated the nation's 911 emergency response network. So far, only four Legion of Doom members have been indicted for the crimes, and none has gone to trial. However, an investigation team

coordinated by Assistant U.S. Attorney William Cook in Chicago and including the secret Service, the U.S. Department of Justice, the FBI and a handful of state attorney generals, has in the past six months raided the homes and businesses of about a dozen suspected legion members across the country. In Austin, Secret Service agents, local police and officers from the University of Texas Police Department seized computer equipment and documents from three homes as part of the probe. One local business, a role-playing game-publishing company called Steve Jackson Games, also was raided in the March crackdown, but officials say the firm is not a primary target of the hacker investigation. The firm is believed to have been raided because investigators wanted to examine equipment used by an employee. The search warrants used in the raids remain sealed from public view, and Secret Service and UTPD officials declined to comment on the case. Law enforcement sources say one of the targets of the Austin investigation is a juvenile who is not believed to be a member of the hacker group. The two other Austinites under investigation are legion members, authorities say, and have been linked to the 911 probe centered in Chicago. According to law enforcement sources, the two men helped circulate information about the 911 system's software through a national bulletin board network that hackers could call by using a telephone, a computer and a modem. In addition, details about ways to tamper with the emergency system were published in Phrack, a legion newsletter. While no one in Austin has been indicted or arrested, officials said they expect some action on the local cases in the next month. And state and federal authorities involved in the national investigation say they are preparing dozens of additional indictments aimed at the entire membership roster of the Legion of Doom. "It doesn't matter whether you commit a burglary by

telephone or by breaking into a building," said Gail Thackeray, an assistant attorney general in Arizona, one of a handful of state investigators working solely on computer crime. "Did they expect that the rest of us would sit by and let every idiot kid in America break into our 911 system?" she said. "I do not respect the right of hackers to learn what they want to learn at the expense of the rest of us." Thackeray, who helped investigate a hacker's attempt to break into the computer system at the Barrow Neurological Institute in Phoenix, said the recent legion crackdown is a result of improved coordination among law enforcement agencies with jurisdiction over computer crime. In addition, she said, the effort has been boosted by a new breed of investigators with computing expertise. Because of the potential for widespread damage to both government and business computer systems, officials say the hacker probe has caught the eye of the Justice Department, which is pushing U.S. attorneys throughout the country to beef up their computer crime-fighting capacity. "There is a push on Capitol Hill to shore up our activity in this area," said an assistant U.S. attorney who asked not to be named. "I think this is the beginning of a boom." Said Thackeray: "There's more computer crime going on out there than any one agency can

handle. We're totally flooded." For members of the Legion of Doom, the unwanted law enforcement attention is nothing new. Formed in 84 and named for a gang at took on Superman and other heroes in the television cartoon Superfriends, the group has survived two other waves of criminal investigations. The first, in 1985, resulted in the Arrrest and conviction of five of the legion's founders for credit card fraud and theft by wire. After a brief resurgence, group members again were arrested en masse in 1987, only to revive again in 88. But according to investigators familiar with the group, pressure form the recent legion crackdown is the most intense to date. Several of the investigators said the legion has shut down, at least for now. A history of the group written by one of its founders and obtained by the Austin American- Statesman seems to bear out investigators' suspicions. The 10- page document recounts significant developments in the group's history, from its founding in 1984 (an event "that would ulti- mately change the face of the computer underground forever," the brochure states), to its current, besieged status. The pamphlet acknowledges that "there is no indication that points to a resurgence in the future" and ends with the words "Legion of Doom (84-90)." The brochure also takes potshots at federal investiga- tors and the media, often accused by legion members of exaggera- ting their crimes and sensationalizing the group. "The Legion of Doom has been called everything from 'organized crime' to a 'communist threat to national security' to an 'international conspiracy of computer terrorists bent on destroying the nation's 911 service,'" the brochure states. "Nothing comes closer to the actual truth than 'bored adolescents with too much spare time.'" Finally, the legion history includes an "alumni" list that conttains the code names of 38 current and former members. According to the legion's own accounting, 14 of the 38 people on the list have either been convicted of computer crimes or are under investigation. Officials familiar with the group say the legion's characterization of itself as a clique of bored whiz kids is inaccurate. Instead, they portray group members as sophisticated and organized malcontents who do not accept conventional concepts of respect and trust. "These are not just wacky kids," Thackeray said. "They have absolute contempt for the rest of us." "They are constantly in a high-level skill kind of game, part of a thrill. They've totally lost touch with reality." William Murray, a systems security fellow for the Ernst & Young accounting firm, said even though hackers take advantage of the tremendous power of personal computers, they still view their crimes as an electronic game of cat and mouse. "This whole sense of excitement and joy is not tempered," Murray said. "Nobody has told them that they have a responsibility for polite behavior." Some states, including Arizona, are developing treatment programs for hackers. Patterned

after Alcoholics Anonymous and drug-treatment centers, the programs are aimed at rehabilitating hackers who have grown dependent on their craft. "It is absolutely addictive behavior," Thackeray said. "When they get their hands on tools as powerful as these computers, they lost all judgement."

Operation "Sun-Devil" by Phreak_Accident
==========

May 9th and 10th brought on two day thats would be marked in every hackers history book. The reason we assume these days will be important to many, is that maybe it's time we opened are eyes and saw the witch hunt currently in progress. In less than 48 hours, 150 Secret Service men and other law officials served 30 search warrents in 14 cities around the nation (This thing was hudge). Operation "Sun-Devil" (As the Attorney General in Phoenix called it), was a success on their part. "The investigation though is not over, and there are more warrents to be executed.", said Jim Folwer of L.A's Secret Service. Any details of the investigation are not being given out at this time. The Asst. Attorney General of Pheonix told Phrack Inc. that there were other problems involving the investigation and that it was an ongoing investigation for the last TWO years. It is my understanding that Gail Thackeray and the Secret Service are not, taking this lightly. She told Phrack inc. that they are not distinquishing pirates, hackers, or phreakers. Basically, it's any kid with a modem that calls a BBS with an alias. Yes, we are the witches, and we are being hunted.

The following are Two news releases obtianed via fax through the U.S. Secret Service for Phrack Inc.

N E W S R E L E A S E
FOR IMMEDIATE RELEASE CONTACT: Gail Thackeray
---------- Assitant Attorney General
May 9, 1990 @ 11:00 A.M. (602) 542-4266

Attorney General Bob Corbin announced today that in connection with an eighteen-month joint investigation into computer crime conducted with the United States Secret Service and the United States Attorney's office, the Arizona Attorney General's office has executed seven search warrants in which computers, electronic bulletin boards, telephone test equipment and records have been seized. The Organized Crime and Racketeering Division investigation involved complaints by Arizona and out of state victims of substantial financial losses resulting from credit card fraud and theft of long distance telephone and data communications services, and by victims of attacks on computer systems operated by government agencies, private corporations, telephone companies, financial institutions, credit bureaus, and a hospital. The Arizona Attorney General's office received information and technical assistance from the Glendale, Arizona Police Department's Computer Crime Unit, and from many private sector sources, including Bellcore (Bell Communications Research), American Express, Communications carriers U.S. Sprint, AT&T, MCI,Com Systems, MidAmerican Communications, LDL Communications, and Shared Use Network. Without the cooperation of these companies and of numerous federal,

state and local law enforcement agencies around the country, this investigation would have been impossible. The privacy of our citizens and the health of our economy depend upon secure, reliable computer systems. Computer fraud and attempts to compromise senstitive public and private computer systems will not be tolerated. Individuals who

commit these offenses in Arizona can expect to be prosecuted.

.end.

P R E S S R E L E A S E

FOR IMMEDIATE RELEASE
Wednesday, May 9, 1990

Contact: Wendy Harnagel
United States Attorney's Office
(602) 379-3011

PHOENIX -- Stephen M. McNamee, United States Attorney District of Arizona,
Robert K. Corbin, Attorney General for the State of Arizona, and Henry R. Potosky, Acting Special Agent in Charge of the United States Secret Service Office in Phoenix, today announced that approximately twenty-seven search warrants were executed on Monday and Tuesday, May 7 and 8, 1990, in various cities across the nation by 150 Secret Service agents along with state and local law enforcement officials. The warrants were issued as a part of Operation Sundevil, which was a two year investigation into alleged illegal computer hacking activities. The United States Secret Service, in cooperation with the United States Attorney's Office, and the Attorney General for the State of Arizona, established an operation utilizing sophisticated investigative techniques, targeting computer hackers who were alleged to have trafficked in and abuse stolen credit card numbers, unauthorized long distance dialing codes, and who conduct unauthorized access and damage to computers. While the total amount of losses cannot be calculated at this time, it is estimated that the losses may run into the millions of dollars. For example, the unauthorized accessing of long distance telephone credit cards have resulted in uncollectible charges. The same is true of the use of stolen credit card numbers. Individuals are able to utilize the charge accounts to purchase items for which no payment is made. Federal search warrants were executed in the following cities: Chicago, IL - Cincinatti, OH - Detroit, MI - Los Angeles, CA Miami, FL - Newark, NJ - New York, NY - Phoenix, AZ - Pittsburgh, PA - Plano, TX - Richmond, VA - San Diego, CA San Jose, CA

Unlawful computer hacking imperils the health and welfare of individuals, corporations and government agencies in the United States who rely on computers and telephones to communicate. Technical and expert assistance was provided to the United States

Secret Service by telecommunication companies including Pac Bel, T&T, Bellcore, Bell South, MCI, U.S. Sprint, Mid-American, Southwestern Bell, NYNEX, U.S. West, and by the many corporate victims. All are to be commended for their efforts for their efforts in researching intrusions and documenting losses. McNamee and Corbin expressed concern that the improper and alleged illegal use of computers may become the White Collar crime of the 1990's. McNamee and Corbin reiterated that the state and federal government will vigorously pursue criminal violations of statutes under their jurisdiction. Three individuals were arrested yesterday in other jurisdictions on collateral or independent state charges. The investigations surrounding the activities of Operation Sundevil are continuing. The investigations are being conducted by agents of the United States Secret Service and Assistant United States Attoryney Tim Holtzen, District of Arizona, and Assistant Arizona Attorney General Gail Thackery.

.end.

RIPCO May 8th, 1990

Operation Sun-Devil claimed more than just a few "Codelords" around the states, it claimed one of the oldest and more popular boards.

Nobody knows when or if RIPCO shall return. Reportedly, Dr. Ripco was charge on a hand-gun violation after his house was searched. Phrack inc. can't comment on this. The following is the exact transcript of the message left on RIPCO's answering maching after Operation Sun-Devil.

- -

This is 528-5020. As you are probably aware, on May 8, the Secret Service conducted a series of raids across the country. Early news reports indicate these raids involved people and computers that could be connected with credit card and long distance toll fraud. Although no arrests or charges were made, Ripco BBS was confiscated on that morning. It's involvement at this time is unknown. Since it is unlikely that the system will ever return, I'd just l say goodbye, and thanks for your support for the last six and a half years. It's been interesting, to say the least.

Talk to ya later.
{Dr. Ricpo}

*** END OF VOICE MESSAGE ***

{C}omputer {E}mergency {R}esponse {T}eam

Some call it "Internet Police" -- Others call it "just stupid." CERT however is a mix. But I do give them credit -- After all, have your number one goal being 'making the Internet more secure' has to be a tough task. Therefore, we give them credit. However,

CERT is funded by DARPA, which is a government agency. And anything in my book that the government runs is bad news. Yes, the government pays the 6 man salary and keep their hot-line active 24 hours a day. Ahh.. What do you know about CERT? "Nothing" you say? Well, the following is the press release and other reprints of information about CERT.

- -

Richard Pethia <rdp@SEI.CMU.EDU>

DEAR XXXXXXXXX,
I have been reviewing our correspondence files and have discovered that your request for information may not have been filled. I apologize for the delay and hope that the information is still useful to you. If, after reading the following, you have additional questions or would like to subscribe to one of our information lists, please send email with your question/request.

The Computer Emergency Response Team (CERT) was established by the Defense Advanced Research Projects Agency in November of 1988 to serve members of the Internet Research community. The press release below describes the general role of the CERT. More specifically, the CERT supports individual Internet sites by: -Working with site personnel to help resolve individual computer security incidents. Contact potentially affected sites to warn them of possible security breaches. Work with sites to change the conditions that allowed incidents to occur. -Issuing advisories that alert the community to specific system vulnerabilities or intrusion techniques, as well as the methods to protect against them. -Working with the community and system (primarily Unix) vendors to reslove specific system vulnerabilities. -Maintaining and operating moderated mailing lists that: (1) provide a discussion forum for tools and techniques to improve the security of Unix systems, and (2) provide a discussion forum and alert mechanism for PC viruses, trojan horses, etc. Over the past year we have developed hundreds of working relationships with members of the Internet and other communities and have established an extensive information

collection and dissemination network. Because of this network of cooperating individuals and organizations, we are often able to advise the community of problems allowing them to take corrective action before being affeceted by those problems.

No. 597-88
(202) 695-0192 (Info.)
(202) 697-3189 (Copies)
IMMEDIATE RELEASE 12 6, 1988 (202) 697-5737 (Public/Industry)

DARPA ESTABLISHES COMPUTER EMERGENCY RESPONSE TEAM

The Defense Advanced Research Projects Agency (DARPA) announced

today that it has established a Computer Emergency Response Team (CERT) to address computer security concerns of research users of the Internet, which includes ARPANET. The Coordination Center for the CERT is located at the Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, PA. In providing direct service to the Internet community, the CERT will focus on the special needs of the research community and serve as a prototype for similar operations in other computer communities. The National Computer Security Center and the National Institute of Standards and Technology will have a leading role in coordinating the creation of these emergency response activities. The CERT is intended to respond to computer security threats such as the recent self-replicating computer program ("computer virus") that invaded many defense and research computers. The CERT will assist the research network communities in responding to emergency situations. It will have the capability to rapidly establish communications with experts working to solve the problems, with the affected computer users and with government authorities as appropriate. Specific responses will be taken in accordance with DARPA policies.

It will also serve as a focal point for the research community for identification and repair of security vulnerabilities, informal assessment of existing systems in the research community, improvement to emergency response capability, and user security awareness. An important element of this function is the development of a network of key points of contact, including technical experts, site managers, government action officers, industry contacts, executive level decision-makers and investigative agencies, where appropriate. Because of the many network, computer, and systems architectures and their associated vulnerabilities, no single organization can be expected to maintain an in-house expertise to respond on its own to computer security threats, particularly those that arise in the research community. As with biological viruses, the solutions must come from an organized community response of experts. The role of the CERT Coordination Center at the SEI is to provide the supporting mechanisms and to coordinate the activities of experts in DARPA and associated communities. The SEI has close ties to the Department of Defense, to defense and commercial industry, and to the research community. These ties place the SEI in a unique position to provide coordination support to the software experts in research laboratories and in industry who will be responding in emergencies and to the communities of potentially affected users.

The SEI is a federally-funded research and development center, operating under DARPA sponsorship with the Air Force Systems Command (Electronic Systems Division) serving as executive agent. Its goal is to accelerate the transition of software technology to defense systems. Computer security is primarily a software

problem, and the presence of CERT at the SEI will enhance the technology transfer mission of the SEI in security-related areas.

-END-

QUESTIONS AND ANSWERS: DARPA ESTABLISHES CERT, 12/6/88

Q: Can you provide background on earlier break-ins?

A: On November 2, 1988, thousands of computers connected to unclassified DoD computer networks were attacked by a virus. Although the virus did not damage or compromise data, it did have the effect of denying service to thousands of computer users. The computer science research community associated with the Defense Advanced Research Projects Agency (DARPA), along with many other research laboratories and military sites that use these networks, quickly responded to this threat. They developed mechanisms to eliminate the infection, to block the spread of the self-replicating program, and to immunize against further attack by similar viruses. Software experts from the University of California at Berkeley, with important contributions from the Massachusetts Institute of Technology and other network sites, rapidly analyzed the virus and developed immunization techniques. These same software experts also provided important assistance in the more recent Internet intrusion of 27-28 November. As the events unfolded, DARPA established an ad hoc operation center to help coordinate the activities of software experts working around the clock and to provide information to appropriate government officials. The operations center had three main tasks. It facilitated communications among the many groups affected, it ensured that government organizations were promptly informed of developments, and it provided initial technical analysis in DoD. Although the threat was contained quickly, a more maliciously designed virus could have done serious damage. The recent events serve as a warning that our necessarily increasing reliance on computers and networks, while providing important new capabilities, also creates new kinds of vulnerabilities. The Department of Defense considers this an important national issue that is of major concern in both the defense and commercial sectors. The DoD is developing a technology and policy response that will help reduce risk and provide an emergency reaction response.

Q: Who will be on the CERT?

A: The CERT will be a team of over 100 experts located throughout the U.S. whose expertise and knowledge will be called upon when needed. When not being called upon, they will continue their normal daily work. As noted in the release, these experts will include: technical experts, site managers, government action officers, industry contacts, executive-level decision-makers and representatives from investigative agencies. recommendations that will be acted upon by DoD authorities.

Q: Is the CERT fully operational now?

A: We are in the very early stages of gathering people for the CERT. We are first concentrating on collecting technical

experts. A staff is in place at SEI, but details are still being worked out.

Q: Will there just be one CERT?

A: The intent is that each major computer community may decide to establish its own CERT. Each CERT will therefore serve only a particular community and have a particular technical expertise. (The DARPA/SEI CERT will serve, for example, the research community and have expertise in Berkeley-derived UNIX systems and other systems as appropriate.) The National Computer Security Center and the National Institute of Standards and Technology will support the establishment of the CERTs and coordinate among them.

Q: What are the special needs of the research community that their CERT will serve?

A: The special challenge of the research community is improving the level of computer security without inhibiting the innovation of computer technology. In addition, as is often DARPA's role, their CERT will serve as a prototype to explore the CERT concept so that other groups can learn and establish their own.

Q: Does the CERT Coordination Center have a press point of contact?

A: No. Their function is to serve as a nerve center for the user community.

.end

USA Today and the devil

Many controversies have been made of the article printed in USA Today after Operation Sun-Devil took it's toll.

Phrack inc. tried to contact the author, and with no luck she wast accepting phone calls. Please remember, this is only a USA Today article -- C'mon, get real USAT.

byline 'Debbie Howlett, USA Today' reads:

A network of computer hackers operating in 14 cities -- which bilked phone companies of $50 million -- has been unplugged, police say.

"We're not talking about somebody who played Space Invaders too many times," says Tim Holtzen, spokesman for the U.S. attorney in Phoenix.

The hackers -- the largest such ring discovered in the USA --broke into phone company and bank computer systems to obtain account numbers and run up an unknown total in debts, police say.

"The main thing is the life-threatening information these computer hackers were trying to get into," says Richard Adams of the Secret Service. "It goes beyond being monetary to totally mischievous."

The ring was uncovered 18 months ago, when members tried and failed to infiltrate computers at Barrows Neurological Institute in Phoenix.

They later tried to block incoming calls to the 911 emergency

service in Chicago. The motivation? "The primary reason is as kind of a malicious hobby." says Gary Chapman of Computer Professionals for Social Responsibility. "People are interested in testing their skills against security measures." But, Adams says, "I hate to minimize it by saying it was just for kicks."

Police seized 40 computers and 23,000 disks during searches Tuesday in 14 cities, officials said Wednesday. Five men, between the ages of 19 and 24, have been arrested.

What's been uncovered so far, says Holtzen, may be "just the tip of the iceberg."

THE ART OF INVESTIGATION By The Butler

There are many ways to obtain information about individuals. I am going to cover some of the investigative means of getting the low down on people whom you wish to know more about.

Some of the areas I will cover are:

Social Security Checks
Driving/Vehicular Records
Police Reports
FBI Records
Insurance Records
Legal Records
Credit Bureau Checks
Probate Records
Real Estate Records
Corporate Records
Freedom Of Information Act
Governmental Agency Records
Maps
Tax Records

To obtain information from some organizations or some individuals one must be able to "BULLSHIT"!!! Not only by voice but in writing. Many times you must write certain governmental bodies requesting info and it can only be done in writing. I can't stress enough the need for proper grammer and spelling.

For you to obtain certain information about another person you must first get a few KEY pieces of info to make your investigation easier. The persons Full Name, Social Security Number, Date &

Place of Birth will all make your search easier and more complete.

First of all in most cases you will know the persons name you want to investigate. If not you must obtain it any way you can. First you could follow them to their home and get their address. Then some other time when they are gone you could look at their mail or dig through their trash to get their Full Name. While in their trash you might even be able to dig up more interesting info like: Bank Accout Numbers, Credit Card Numbers, Social Security Number, Birth Day, Relatives Names, Long Distance Calls Made, etc.

If you can't get to their trash for some reason take their address to your local library and check it against the POLKS and COLES Directories. This should provide you with their Full Name, Phone Number, Address, and how long they have lived at the current location.

You can also check the Local Phone Book, Directory Assistance,

City Directories, Post Office, Voter Registration, Former Neighbors, Former Utilities (water, gas, electric, phone, cable, etc.)

If you know someone who works at a bank or car dealer you could have them run a credit check which will reveal all of their credit cards and if they have ever had any late payments or applied for any loans. If you are brave enough you could even apply for a loan impersonating the individual under investigation The Credit Bureau also has Sentry Services that can provide deceased social security numbers, postal drop box address and known fraudulent information.

You can get an individuals driving record by sending a letter to your states Department of Revenue, Division of Vehicles. You can also get the following:

Driver Control Bureau For Driving Record send Name, Address, Date of Birth and usually a $1 processing fee for a 5 year record.

Titles & Registration Bureau For ownership information (current and past).

Driver License Examination Bureau To see what vision was rated.

Motor Carrier Inspection & Registration Bureau To check on licensing and registration of trucks/trucking companies.

Revocation Dept Can verify if someone's driver's license has ever been suspended or revoked.

You can even obtain a complete vehicle history by sending the vehicle description, identification # for the last registered owner, and a small fee. Send this info to your states Dept of Vehicles. It is best to contact them first to get their exact address and fees. I would advise using a money orders and a P.O. Box so they cannot trace it to you without a hassle.

Police Records

All Police and Fire Records are Public record unless the city is involved. You can usually get everything available from the police dept including: Interviews, maps, diagrams, misc reports, etc.

FBI Records

If the individual you are inquiring about is deceased the FBI will

provide some info if you give them Full Name, SSN, Date & Place of Birth. Contact you local FBI office to get the details.

Real Estate Records

Recorder of Deeds offices in each county maintain land ownership records. Most are not computerized and you have to manually search. Then you must review microfilm/fiche for actual deeds of trust, quit claim deeds, assignments, mortgage, liens, etc.

A title company can run an Ownership & Equity (O&E) search for a fee ($80-$100) which will show ownership, mortgage info, easements, taxes owned, taxes assessed, etc.

Most county assessors will provide an address and value of any real property if you request a search by name.

Social Security Records

Social Security Administrator
Office of Central Records Operations
300 North Greene Street
Baltimore, Maryland 21201
301-965-8882

Title II and Title XVI disability claims records, info regarding total earnings for each year, detailed earnings information show employer, total earnings, and social security paid for each quarter by employer.

Prices are approximately as follows:

1st year of records	$15.00
2nd-5th year of records	$ 2.50 per person
6th-10th year of records	$ 2.00 per person
11th-15th year of records	$ 1.50 per person
16th-on year of records	$ 1.00 per person

** Call for verification of these prices. **

Social Security records are a great source of information when someone has been relatively transient in their work, or if they are employed out of a union hall.

If you want to review a claim file, direct your request to the Baltimore office. They will send the file to the social security office in your city for you to review and decide what you want copies of.

The first three digits of a social security number indicate the state of application.

The Social Security Number

SSA has continually emphasized the fact that the SSN identifies a particular record only and the Social Security Card indicates the person whose record is identified by that number. In no way can the Social Security Card identify the bearer. From 1946 to 1972 the legend "Not for Identification" was printed on the face of the

card. However, many people ignored the message and the legend was eventually dropped. The social security number is the most widely used and carefully controlled number in the country, which makes it an attractive identifier.

With the exception of the restrictions imposed on Federal and some State and local organizations by the Privacy Act of 1974, organizations requiring a unique identifier for purposes of controlling their records are not prohibited from using (with the consent of the holder) the SSN. SSA records are confidential and knowledge of a person's SSN does not give the user access to information in SSA files which is confidential by law.

Many commercial enterprises have used the SSN in various promotional efforts. These uses are not authorized by SSA, but SSA has no authority to prohibit such activities as most are not illegal. Some of these unauthorized uses are: SSN contests; skip-tracers; sale or distribution of plastic or metal cards; pocketbook numbers (the numbers used on sample social security cards in wallets); misleading advertising, commercial enterprises charging fees for SSN services; identification of personal property.

The Social Security Number (SSN) is composed of 3 parts, XXX-XX-XXXX, called the Area, Group, and Serial. For the most part, (there are exceptions), the Area is determined by where the individual APPLIED for the SSN (before 1972) or RESIDED at time of application (after 1972). The areas are assigned as follows:

000	unused	387-399	WI	528-529	UT
001-003	NH	400-407	KY	530	NV
004-007	ME	408-415	TN	531-539	WA
008-009	VT	416-424	AL	540-544	OR
010-034	MA	425-428	MS	545-573	CA
035-039	RI	429-432	AR	574	AK
040-049	CT	433-439	LA	575-576	HI
050-134	NY	440-448	OK	577-579	DC
135-158	NJ	449-467	TX	580	VI Virgin Islands
159-211	PA	468-477	MN	581-584	PR Puerto Rico
212-220	MD	478-485	IA	585	NM
221-222	DE	486-500	MO	586	PI Pacific Islands*
223-231	VA	501-502	ND	587-588	MS
232-236	WV	503-504	SD	589-595	FL
237-246	NC	505-508	NE	596-599	PR Puerto Rico
247-251	SC	509-515	KS	600-601	AZ

252-260	GA	516-517	MT	602-626	CA
261-267	FL	518-519	ID	*Guam, American Samoa,	
268-302	OH	520	WY	Northern Mariana Islands,	
303-317	IN	521-524	CO	Philippine Islands	
318-361	IL	525	NM		
362-386	MI	526-527	AZ		

627-699 unassigned, for future use
700-728 Railroad workers through 1963, then discontinued
729-899 unassigned, for future use
900-999 not valid SSNs, but were used for program purposes when state aid to the aged, blind and disabled was converted to a federal program administered by SSA.

As the Areas assigned to a locality are exhausted, new areas from the pool are assigned. This is why some states have non-contiguous groups of Areas. The Group portion of the SSN has no meaning other than to determine whether or not a number has been assigned. SSA publishes a list every month of the highest group assigned for each SSN Area. The order of assignment for the Groups is: odd numbers under 10, even numbers over 9, even numbers under 9 except for 00 which is never used, and odd numbers over 10. For example, if the

highest group assigned for area 999 is 72, then we know that the number 999-04-1234 is an invalid number because even Groups under 9 have not yet been assigned.

The Serial portion of the SSN has no meaning. The Serial is not assigned in strictly numerical order. The Serial 0000 is never assigned.

Before 1973, Social Security Cards with pre-printed numbers were issued to each local SSA office. The numbers were assigned by the local office. In 1973, SSN assignment was automated and outstanding stocks of pre-printed cards were destroyed. All SSNs are now assigned by computer from head-quarters. There are rare cases in which the computer system can be forced to accept a manual assignment such as a person refusing a number with 666 in it.

A pamphlet entitled "The Social Security Number" (Pub. No.05-10633) provides an explanation of the SSN's structure and the method of assigning and validating Social Security numbers.

Tax Records

If you can find out who does the individuals taxes you might be able to get copies from them with the use of creative social engineering. If you want to run a tax lien search there is a service called Infoquest. 1-800-777-8567 for a fee. Call with a specific request.

Post Office Records

If you have an address for someone that is not current, always consider writing a letter to the postmaster of whatever post office branch services the zip code of the missing person. Provide them the name and the last known address and simply ask for the current address. There might be a $1 fee for this so it would be wise to call first. City Directory, Polk's, Cole's, etc. Information in these directories is contained alphabetically by name, geographically by street address, and numerically by telephone number, so if you have any of those three pieces of info, a check can be done. The Polk's directory also shows whether the person owns their home or rents, their marital status, place of employment, and a myriad of other tidbits of information. However, these books are not the be-all and end-all of the information as they are subject to public and corporate response to surveys. These directories are published on a nationwide basis so if you are looking for someone outside of your area, simply call the public library in the area you have an interest and they also can perform a crisscross check for you.

You can also call a service owned by Cole's called the National Look up Library at 402-473-9717 and either give a phone number and get the name & address or give the address and get the name and phone number. This is only available to subscribers, which costs $183.00 dollars for 1991. A subscriber gets two free lookups per day and everyone after that costs $1.25. A subscriber can also mail in a request for a lookup to:

National Look Up Library
901 W. Bond Street
Lincoln, NE 68521-3694

A company called Cheshunoff & Company can, for a $75 fee, obtain a 5-year detailed financial analysis of any bank.

505 Barton Springs Road
Austin, Texas 78704
512-472-2244

Professional Credit Checker & Nationwide SSN-locate.

!Solutions! Publishing Co.
8016 Plainfield Road
Cincinnati, Ohio 45236
513-891-6145
1-800-255-6643

Top Secret Manuals

Consumertronics
2011 Crescent Drive
P.O. Drawer 537-X
Alamogordo, New Mexico 88310
505-434-0234

Federal Government Information Center is located at

1520 Market Street
St. Louis, Missouri
1-800-392-7711

U.S. Dept of Agriculture has located aerial photos of every inch of the United States.

2222 West 2300 S.
P.O. Box 36010
Salt Lake City, Utah 84130
801-524-5856

To obtain general information regarding registered agent, principals, and good standing status, simply call the Corporate Division of the Secretary of State and they will provide that information over the phone. Some corporate divisions are here:

Arkansas Corporate Division	501-371-5151
Deleware Corporate Division	302-736-3073
Georgia Corporate Division	404-656-2817
Indiana Corporate Division	317-232-6576
Kansas Corporate Division	913-296-2236
Louisiana Corporate Division	504-925-4716
Missouri Corporate Division	314-751-4936
New York Corporate Division	518-474-6200
Texas Corporate Division	512-475-3551

Freedom Of Information
The Freedom of Information Act allows the public to request information submitted to, or generated by, all executive departments, military departments, government or government controlled corporations, and regulatory agencies. Each agency, as described above, publishes in the Federal Register, descriptions of its central and field organizations and places where and how requests are to be directed. Direct a letter to the appropriate person designated in the Federal Register requesting reasonably described records be released to you pursuant to the Freedom of Information Act. Be sure to follow each agency's individually published rules which state the time, place, fees, and procedures for the provisions of information. The agency should promptly respond.

How to Find Information About Companies, Ed. II, 1981, suggests, "Government personnel you deal with sometimes become less helpful if you approach the subject by threatening the Freedom of Information Act action - it's best to ask for the material informally first." While this will probably enable you to find the correct person to send your request to, be prepared to spend at least half an hour on the phone talking to several people before you find the person who can help you. The book also has a brief description of what each governmental agency handles.

If you want to see if someone you are trying to locate is a veteran, has a federal VA loan, or receives some sort of disability benefit, use Freedom of Information and provide the person's SSN.

You will get a bill but you can ask for a fee waiver if this contributes to a public understanding of the operation of the government. You can also request an opportunity to go through the files yourself and then decide what you want copied.

Insurance Records

PIP carrier records (may contain statements, medical records, new doctors/hospital names, records of disability payments, adjuster's opinions, applications for insurance coverage, other claim info, etc.)

Health insurance records (may contain medical records, record of bills, new doctors/hospital names, pre-existing conditions information, info regarding other accidetns/injuries, etc.)

Often you will have to go through the claims office, the underwriting dept, and the business office to get complete records as each individual dept maintains its own seperate files.

Workers Compensation

Some states will let you simply request records. Just submit your request including the SSN and Birthdate, to the Department of Human Resources, Division of Worker's Compensation. They will photocopy the records and send you the copies. Other states require an authorization to obtain these records.

You can always call your local Private Investigator pretending you are a student doing a research paper on the methods of getting personal information about people or even trash his place to find tips on tracking down people.

Frankie's Fireside Phreak Primer
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
A few words of advice that apply to phreaks every-where. Whether a telecom veteran, or a KOdez Kid, the following guidelines may keep you out of trouble and make life in the Computer Underground a little more pleasant. Brought to you by the CULT, o'course.

>> A CULT Publication by High Priest and Scribe, Franken Gibe <<
-cDc- Cult of the Dead Cow Dissemination Council -cDc-
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

=+=+=+

these. When an IC owns its own carrier, it receives KP + II + 10Dig (YOUR phone number) + ST. In other words, these guys are generally ANI equipped. How can you tell? Well, if you've got an 800 access port, and the exchange is NXX (i.e., you've got a number :1-800-NXX-XXXX), then FIRST dial 1-800-NXX-0000. If you get the "You have reached the AT&T Long Distance Network" recording, the # is AT&T. If you get a "Your call cannot be completed " recording, DO NOT use that WATS number. Simple.

6) [or whatever number...sigh] PLEASE...for your own good, and that of Phreakdom, DO NOT advertise what you do. Yeah, some kids at school might think it's pretty k-radical. Those same kids are the ones to nark, or to mention stuff to the friendly administrators should they ask around. The less non-phreaks know the better. Keep your MOUTH SHUT.

That reminds me of poor Disk Demon [of 915]. The kid really wasn't expecting trouble, but he made the fatal mistake of talking: probably to someone he trusted, and probably he didn't say much. All he mentioned was bringing a pirated disk to school the next day over the phone which was all the cops needed to search his house, and bam...they have him with telecom fraud evidence. The cops don't need much to get a warrant to monitor your telfo. It's a scary reality in a nation that takes less and less seriously the Bill of Rights.

8) NEVER phreak voice calls. Sigh. I know, I'm sure there are a thousand screams of "Oh, COME ON, that's going too far". Okay, let me qualify that, then. Voice-phreak only if you're 1) sure you're not monitored (and who is ever sure?) and 2) know that the recipient can handle possible threats and unpleasantness from the friendly operator who may give him a buzz. Feds and investigators ain't stupid...or at least, not THAT stupid. As long as no one admits anything, it's okay. But the minute you start voice-phreaking, you open a lot of loose ends. Some suggestions, then, for voice phreaking:

   A) Try to remain anonymous. Not too hard.
   B) IF you're talking to strangers, don't mention where you're calling from, much less leave a number. Yeah, just common sense.
   C) Don't talk about phreaking over the line if you don't think the line is secure. Duh!
   D) If you trust the kid you're calling, tell him you've phreaked a call to him. Ask him if it's "cool". Make sure he can handle possible (and usually improbable) inquiries. Make sure his 'rents know NOTHING.

9) That's another thing. This doesn't have to do with safe phreaking, but with keeping phreaks safe. Know what you'll say if you ever get called by an operator or investigator type. If you have a bbs or data line, great. If not, have a story ready and rehearsed. When you think about it, it IS kinda hard for these people to believe that you don't know WHO called you for 5 hours last Sunday night...be prepared. (Ee! Boy scouts rule.)

This file was just to be a short set of definitions for those of you who don't know all the phreaking terms. This was requested by a few people on a small 312 board called The Magnetic Field Elite (312-966-0708, call, board has potential) like The Don. But I have decided against making this small file that is common in many places but instead to make something that I have never seen before. Not just a common file but one of high technical use.

With a printout of this you will never need to missout on a definition again. But that's not all. The file will discuss, indepth, the working of each of these operations below. If you are viewing this file simply for the sake of finding one meaning I suggest that you get the entire thing and then never need to call and view phreak files again.

Topic 1: The Phone/Modem

Scince phreaking is impossible without a phone or modem you I will start with the most important and most complex part of phreaking. The Phone. Now, the phone is a device that transfer sounds as sound enters a receiver, is transfered to an amount of

voltage, sent through the telephone lines and decode back to sound. A modem is based on a universal language of sounds transfered through the modem. Modem stands for the work Modulator/Demodulator. This is like receiveing and sending. Now, with most modems, before connecting, tones just are just the same as the tones that a common phone can make. But the phone can make many tones and some have purposes that are very useful, tones that are reserved for At&t, and thus dangerous. To go through all the tone would be senseless and a book on tones alone could be written (Hmm...maybe I could...) so I will not go into that. But, assuming that you know what a box is I will explain what the odd types of modems can do. If you own an Apple Cat modem you may use it to generate any tone. This is very useful. Some people are against the Cat for various. I will remain neutral on the topic but if you have no understand then phreak the way you see easiest and safest. The ther way is by using an acoustic modem. You may modify a phone to make certain tones and you may make then send these tones through the acoustic modem by placing the headset of the phone on the acoustic's couplers. You may also attempt to make the box modfications directly to the modem but if you error and damage the modem alot of money is wasted while you could have used an acoustic and messed up a twenty dollar phone. Basicaly the common phone can make 18 tones. For example, when you press a number on the phone two tones are made together and make the signal for the number or charater you hit. This is the entire phone to line explantion of the phone. Now the actual internal working of the phone is very complex and can be best under stood by getting a book from the library on it.

Topic 2: The Calling of Numbers

When you call a local number as soon as you hit a number other than one you the phone knows that you are calling localy. Once seven digits are entered the numbers are sent to the nearest switching station and you call goes out. The station deter mines the units per minute and start billing as soon as the called phone answers. All calls are automaticaly one minute long. If you hit a one as the first digit you dial the phone recignizes this as a long distance call and sends you to either the At&t switching station or to another long distance service if you have chose to use other than At&t. If you are using a At&t the call goes through the long distance switching station where unit per minute is determined and then it is refured to the number you called. The call may be slowed down depending on how many times the switching station changes between you and the place you are calling. If it changes between ESS and X-Bar (described below) one it would go through fast. If it changed between them 50 times it would be a very slow call going through. Plus the sound quality may decrease but that is not a fact, just an understanding I have come to when callign long distance with At&t. If you are calling through any other service, such as MCI, Alnet, Teleco, US Sprint or any of the other endless companies,

then things are not the same for long distance calls. You call first goes to the company you call through and price of call is determined by any of the ways a company determines price. The call then goes out through the lines to the long distance companie's station nearest to the number you dialed and tres to go though. If the number is too far away from a station you may get a "The number you have dialed cannot be reached from your calling area." Thus, you have the basic information of how call goes out. Now to get to phreaking and the real reson you read this file.

Topic 3: The Long Distance Company and Codes.

The way of using a different long distance company or not paying a quarter when calling from a payphone. Using the phone card or the code.Names for these numbers: 950's, 800's, Extenders, PBX's, 950 ports, Port, Code port, (Company name) port

The above mentioned names are the phreaks lifeline. They are places where you call and enter a code, then the area code of the place you want to call and finally the number for the place you want to call. When the code is entered it is checked if it is valid and then the person how owns the code pays for the call. If the code is not valid you normaly get a message saying that the code you entered is not valid. When a call goes through it is the same as a normal long distance call except that it is charged to the owner of the card. Some places may require that you enter a nine or a one before you enter the code. Now, the phreak uses these places by calling them over and over again until they get a code. But they do this with a computer and a program such as Hack-a-Matic, Hacking Construction Set (often called HCS), Hack This Buddy, Intellihacker (Old), C at-(and then a name, for the Apple Cat. Has to many names to list), and some others. These are all Apple programs but there are also code hackers for the Commodor 64, 128, Amiga, IBM (of course) and so on. Most computers have them. One thing I have found useful is to use a Radio Shack portable computer with a built in modem and hack from other houses, this is much safer. Secrity in these companies run from really tough (MCI) to sad (like the places that tryo to scare off hackers with tape recordings). 950 ports in the ESS area are set up to trace and could do so very easily but for some reson they are against it. Possibly the time and modey to cheack the calls and pay for tracing. Places have gotton tougher though, if three people get busted off a number in one week and this has never happened before then you can almost be sure that they have stepped up security and that it is time to use a new port.

Now I will discuss some of the things used by the Phreak.

Topic 4: The Loop

Loops, although they may seem fun they are really rather useless. They work as follows. Two numbers are looped together. Usually they are almost the same just a digit different from one another. If you call the lower number you will wait a few secounds and then hear a 1000mhz. tone. If you call the higher number you will hear nothing. If you can one number (dosen't matter which) and someone else calls the other number you will be able to talk to each other. The purpose of these is to test trunk lines. This way they could make sure there was no break in each trunk. Now the old purpose for loops was that they where free to call so one person would call one and another would call the other and they would get to talk for

free. Also, one person might call one number and just wait and talk to whoever called the other number. Like a two line bridge. Today you cannot call these without being charged because the phone company caught on. But you can split a phone call with these so if there is a loop between you and a person you want to talk to you can only pay for half by calling the loop. And the phone company dosen't care because either way they get their money. The billing service for a loop is one all by itself, not like normal local calling and for this reson I might almost belive the rumor that Blue Box tones can be used to call loops. The loops billing service didn't exist awhile back so a call to one was free. Now, if you call this new billing system picks it up. But the loops billing system is just something that At&t scraped together and there are most likly some holes in the system (like not recording blue box tone generation numbers).

Topic 5: The Diverter

The diverter has been a very simple, yet incredibly usefulthing through the years. To use one you must call, after hours and let someone answer the phone, don't answer them, let them hang up and get a faint dialtone. Then you dial again and call from the diverter. Before, you could use a diverter and call through it. The you would only be charged for the call to the diverter, not the one after it. That bill went to the diverter itself. But they fix this problem easily and now you still get charged if you are in the ESS area. Also before, you could use a diverter to call a number that traces and instead of being traced to your number it is traced to the diverter. But ESS eliminated that too. But you can still use a diverter to call hard to reach numbers. Like if you called a place and it gave you a "The number you have dial cannot be reach from your calling area" then if you knew of a diverter in the area of the number you could call through it to the unreachable number and get through. The way a diverter works is after hours when you call a place the call is forwarded to another place. Then, when you don't answer the person at the other place hangs up and your call tries to disconnect from the forwared number and you end up at the diverter with it's dialtone.

HACKING TYMNET

AS MOST OF YOU ALREADY KNOW, TYMNET IS AN INFORMATION SYSTEM ACCESSABLE BY COMPUTERS WITH MODEMS FROM ALMOST ANYWHERE IN THE COUNTRY. TYMNET INCLUDES MANY SUB-SYSTEMS OF INFORMATION WHICH CAN BE USEFUL FOR BUSINESSES OR JUST PHUN. ONE SUB-SYSTEM WHICH I WILL WRITE A SEPARATE ARTICLE ON IS THE ATPCO'S ELECTRONIC TARIFF SYSTEM. BUT FOR NOW, I'LL MAKE ALL OF YOU EXPERTS IN TYMNET SO YOU CAN HAVE AS MUCH PHUN AS YOURS TRUELY.

ACCESS NUMBERS

FOR YOUR LOCAL ACCESS NUMBER YOU COULD CALL THE NICE PERSON AT 800-336-0149 AND REQUEST IT FOR YOUR AREA. IF YOU LIVE NEAR A METROPOLITAN AREA ASK FOR THAT AREA CODE SINCE THEY RARELY HAVE ACCESS NUMBERS FOR OUT-OF-CITY AREAS. FOR THOSE OF YOU IN THE 914 AREA YOU CAN USE: POUGHKEEPSIE : 914-473-0401 WHITE PLAINS : 914-684-6075

LOGGING IN TO TYMNET
---

1. WHEN YOU HAVE CONNECTED WITH THE NETWORK, THE FOLLOWING REQUEST WILL BE DISPLAYED: PLEASE TYPE YOUR TERMINAL IDENTIFIER ENTER YOUR TERM.IDENTIFIER ACCORDING TO THE FOLLOWING CHART:

KEY: IDENT = IDENTIFIER
ASC = ASCII

EBCD = EBCD CORRESPONDENCE
<R> = CARRIAGE RETURN

SPEEDS ARE GIVEN IN CPS (CHARACTERS PER SECOND). TO TRANSLATE TO BAUD RATE JUST MULTIPLY BY 10.

IDENT	CODE	SPEED	TERMINAL TYPE
A	ASC	30,120 WITH CRT	PERSONAL COMP.
B	ASC	15	ALL TERMINALS
C	ASC	30	IMPACT PRINTMRS
D	ASC	10	ALL TERMINALS
E	ASC	30	THERMAL PRINTERS
F	ASC	15 IN 30 OUT	BETA TERMINALS
G	ASC	30,120	BELT PRINTERS G.E. TERMINET
I	ASC	120	MATRIX PRINTERS
P<R>	EBCD	14.8	SELECTRIC-TYPE TERMINALS (E.G., 2741)

[MOST EVERYBODY AT HOME WILL USE THIS OPTION SO IF YOU AREN'T SURE USE A]

IF THE MESSAGE DOES NOT APPEAR JUST WAIT A FEW SECONDS THEN ENTER IT. NOTE THAT ONLY P IDENTIFIERS NEED A <R> THEM BUT SINCE MOST OF YOU WON'T BE USING P FORGET IT.

2. TYMNET WILL THEN DISPLAY THE NUMBER OF THE REMOTE ACCESS NODE TO WHICH YOU ARE CONNECTED, FOLLOWED BY THE NUMBER OF YOUR PORT ON THE NODE, AND WILL DISPLAY THIS REQUEST:

```
-NNNN-PPP-
PLEASE LOG IN:
```

3. TYPE YOUR USER NAME AND <R> THIS USER NAME SEEMS TO BE THE ABBREVIATION FOR THE COMPANY WHO OWNS THE SUB-SYSTEM. FOR EXAMPLE, FOR ELECTRONIC TARIFF THE USER NAME
IS ATP WHICH STANDS FOR AIRLINE TARIFF PUBLISHING, THE COMPANY THAT RUNS THE ELECTRONIC TARIFF.

4. TYMNET WILL THEN REQUEST:

```
PASSWORD:
```

TYPE YOUR PASSWORD AND <R>. THE PASSWORD MAY NOT BE DISPLAYED ON YOUR SCREEN.

5. TYMNET WILL THEN DISPLAY SOME CHARACTER OR MESSAGE INDICATING THAT YOU HAVE LOGGED ON. SINCE BUSINESSES DON'T REALLY GET COMPLICATED WITH PASSWORDS AND THE SUCH, JUST ENTER VALID USER NAMES AND FOR PASSWORDS YOU CAN FORGET CTRL-CHARACTERS... PASSWORDS HAVE A LENGTH OF 8 CHARACTERS (AS FAR AS I KNOW).

TYMNET CONTROL CHARACTERS

CTRL-CHAR	OPERATION
H	HALF-DUPLEX
P	EVEN PARITY
R	ALLOWS THE TERMINAL TO CONTROL THE INCOMING FLOW OF DATA WITH X-ON/OFF CHARACTERS (SEE BELOW)

S X-OFF CHARACTER
Q X-ON CHARACTER

ACCESSING DATAPAC

THE STANDCRD PROCEDURE FOR ACCESSING A HOST ON THE DATAPAC NETWORK IS DESCRIBED BELOW. TYMNET'S INFORMATION DIRECTORY INCLUDES FILES OF MATERIAL ABOUT DATAPAC AND TYMNET'S INTERNATIONAL SERVICES.

LOGGKNG IN TO DATAPAC
---

1. DIAL-UP TYMNET (SEE ABOVE)

2. ENTER YOUR TERMINAL IDENTIFIER

3. AT THE "PLEASE LOG IN:" PROMPT, ENTER THE LOG-IN COMMAND, SPECIFYING: THE DATAPAC NETWORK (DPAC), A SEMICOLON (A SECOND SEMICOLON WILL ECHO AT YOUR END) , THE DATAPAC NETWORK IDENTIFICATION CODE (3020), THE 8-DIGIT HOST ADDRESS AND <R>.

E.G., DPAC;;3020HOST ADDRESS <R>

IF YOU NEED TO ENTER FUTHER USER DATA ENTER A COLON AFTER THE HOST ADDRESS THEN A <R>.

E.G., DPAC;;3020HOST ADDRESS:USER DATA <R>

5. DATAPAC WILL THEN DISPLAY A MESSAGE OR CHARACTER TO SHOW THAT YOU ARE ON-LINE.

THIS LITTLE BIT OF INFORMATION SHOULD GET SOME OF YOU GOING. MY EXPERIENCES WITH TYMNET HAVE BEEN MAINLY RESTRICTED TO THE ATPCO SYSTEM SO COMMANDS MAY DIFFER.

THE PHREAKER'S HANDBOOK #1 by Phortune 500

a useful source for the phreaker covering both the basics and advances of phreaking

GENERAL NOTE

The purpose of this newsletter is purely educational. It has been released in order to teach and advance the knowledge of today's declining phreaks. However, the author does not take any responsibility over the misuse of the herein contained information, and the newsletter itself does not encourage or support the above type of activity. Also, any wrong or old information in this document is not to the responsibility of the author, and the reader accepts any consequences due to information that may be mistaken in this manner.

NOTE TO ABUSERS

All information contained within this document was intended towards educational purposes. Any misuse or illegal use of the information contained in this document is strictly at the misuser's risk. The author assumes NO responsibility of the reader's actions following the release this document (in otherwords, you're on your own if you get nailed!)

TPH Issue #1, Volume 1 Release Date::July 3, 1989

Introduction To TPH #1

This phile was written for beginning as well as those uninformed "advanced" phreaks who need something as a reference when reading or writing philes concerning phreaking or fone phraud. Of course, you could be a beginning phreak and use this phile to B.S. your way into a big group by acting like you know a lot, or something, but that is up to you. Anyway, I compiled this listing phrom various sources, the majority is listed as references at the end of this phile.

This phile's only goal is to educate and inform. Any illegal or fraudulent activity is neither encouraged nor supported by the author of this phile, not by the majority of the >TRUE< phreaking community. The author assumes NO responsibility for the actions of the reader.

Also, I know that some of the stuff covered in this release of TPH will be old and outdated; however, I will try to clean that up by the next release of TPH, and will notify you, the reader, of the changes due to these revisions.

The Phreak's Vitals:

True Definition Of The Phreaker

"Many people think of phone phreaks as slime, out to rip off Bell for all she is worth. Nothing could be further from the truth! Granted, there are some who get their kicks by making free calls; however, they are not true phone phreaks. Real phone phreaks are 'telecommunications hobbyists'who experiment, play with, and learn from the phone system. Occasionally, this experimenting and a need to communicate with other phreaks, without going broke, leads to free calls. The free calls are but a small subset of a >TRUE< phone phreak's activities."

- Wise Words Of The Magician

The Phone Phreak's Ten Commandments

I. Box thou not over thine home telephone wires, for those who doest will surely bring the wrath of the Chief Specialent down upon thy head.
II. Speakest thou not of important matters over thine home telephone wires, for to do so is to risk thine right of freedom.
III. Use not thine own name when speaking to other phreaks, for that every third phreak is an FBI agent is well known.
IV. Let not overly many people know that thy be a phreak, as to do so is to use thine own self as a sacrificial lamb.
V. If thou be in school, strive to get thine self good grades, for the authorities well know that scholars never break the law.
VI. If thou workest, try to be an employee and impressest thine boss with thine enthusiasm, for important employees are often saved by their own bosses.
VII. Storest thou not thine stolen goodes in thine own home, for those who do are surely non-believers in the Bell System Security Forces, and are not long for this world.
VIII. Attractest thou not the attention of the authorities, as the less noticeable thou art, the better.
IX. Makest sure thine friends are instant amnesiacs and willst not remember thou hast called illegally, for their cooperation with the authorities willst surely lessen thine time for freedom on this earth.
X. Supportest thou TAP, as it is thine newsletter, and without it, thy work would be far more limited.

The Phreaker's Glossary

1XB - No.1 Crossbar system. See XBAR for more information.

2600 - A hack/phreak oriented newsletter that periodically was released and still is being released. See Phile 1.6 for more information on the magazine and ordering.

4XB - No.4 Crossbar system. See XBAR for more information.

5XB - No.5 Crossbar system. The primary end office switch of Bell since the 60's and still in wide use. See XBAR for more detail.

700 Services - These services are reserved as an advanced forwarding system, where the forwarding is advanced to a user-programed location which could be changed by the user.

800 Exceptional Calling Report - System set up by ESS that will log any caller that excessively dials 800 numbers or directory assistance. See ESS for more information.

800 Services - Also known as WATS. These services often contain WATS extenders which, when used with a code, may be used to call LD. Many LD companies use these services because they are toll-free to customers. Most 800 extenders are considered dangerous because most have the ability to trace.

900 Services - Numbers in the 900 SAC usually are used as special services, such as TV polls and such. These usually are $.50 for the first minute and $.35 for each additional minute. Dial (900)555-1212 to find out what the 900 services currently have to offer.

950 - A nationwide access exchange in most areas. Many LD companies have extenders located somewhere on this exchange; however, all services on this exchange are considered dangerous due to the fact that they ALL have the ability to trace. Most 950 services have crystal clear connections.

ACCS - Automated Calling Card Service. The typical 0+NPA+Nxx+xxxx method of inputting calling cards and then you input the calling card via touch tones. This would not be possible without ACTS.

ACD - Automatic Call Distributor.

ACD Testing Mode - Automatic Call Distributor Test Mode. This level of phreaking can be obtained by pressing the "D" key down after calling DA. This can only be done in areas that have the ACD. The ACD Testing Mode is characterized by a pulsing dial tone. From here, you can get one side of a loop by dialing 6, the other side is 7. You may also be able to REMOB a line. All possibilities of the ACD Test have not been experimented with. See silver box for more details.

ACTS - Automated Coin Toll Service. This is a computer system that automates phortress fone service by listening for red box tones and takes appropriate action. It is this service that is commonly heard saying, "Two dollars please. Please deposit two dollars for the next three minutes." Also, if you talk for more than three minutes and then hang up, ACTS will call back and demand your money. ACTS is also responsible for ACCS.

Alliance - A teleconferencing system that is apart from AT&T which allows the general public to access and use its conferencing equipment. The equipment allows group conversations with members participating from throughout the United States. The fone number to Alliance generally follows the format of 0-700-456-x00x depending on the location the call originates from and is not accessible direct by all cities/states.

AMA - Automated Message Accounting. Similar to the CAMA system; see CAMA for more info.

analog - As used for a word or data transmission, a continuously varying electrical signal in the shape of a wave.

ANI - Automatic Number Identification - This is the system you can call, usually a three digit number or one in the 99xx's of your exchange, and have the originating number you are calling from read to you by a computer. This is useful if you don't know the number you are calling from, for finding diverters, and when you are playing around with other fone equipment like cans or beige boxes. The ANI system is often incorporated into other fone companies such as Sprint and MCI in order to trace those big bad phreaks that abuze codez.

ANIF - Automatic Number Identification Failure. When the ANI system of a particular office fails.

APF - All PINs Fail. This is a security measure which is designed to frustrate attempts at discovering valid PINs by a hacking method.

aqua box - A box designed to drain the voltage of the FBI lock-in- trace/trap-trace so you can hang up your fone in an emergency and phrustrate the Pheds some more. The apparatus is simple, just connect the two middle wires of a phone wire and

plug, which would be the red and green wires if in the jack, to the cord of some electrical appliance; ie, light bulb or radio. KEEP THE APPLIANCE OFF. Then, get one of those line splitters that will let you hook two phone plugs into one jack. Plug the end of the modified cord into one jack and your fone into the other. THE APPLIANCE MUST BE OFF! Then, when the Pheds turn their lame tracer on and you find that you can't hang up, remove your fone from the

jack and turn the appliance ON and keep it ON until you feel safe; it may be awhile. Then turn it off, plug your fone back in, and start phreaking again. Invented by: Captain Xerox and The Traveler.

BAUDOT - 45.5 baud. Also known as the Apple Cat Can.

BEF - Band Elimination Filter. A muting system that will mute the 2600 Hz tone which signals hang-up when you hang up.

beige box - An apparatus that is a home-made lineman's handset. It is a regular fone that has clips where the red and green wires normally connect to in a fone jack. These clips will attach to the rings and tips found in many of MA's output devices. These are highly portable and VERY useful when messing around with cans and other output devices the fone company has around. Invented by: The Exterminator and The Terminal Man.

BITNET - Nationwide system for colleges and schools which accesses a large base of education-oriented information. Access ports are always via mainframe.

bit stream - Refers to a continuous series of bits, binary digits, being transmitted on a transmission line.

black box - The infamous box that allows the calling party to not be billed for the call placed. We won't go in depth right now, most plans can be found on many phreak oriented BBS's. The telco can detect black boxes if they suspect one on the line. Also, these will not work under ESS.

bleeper boxes - The United Kingdom's own version of the blue box, modified to work with the UK's fone system. Based on the same principles. However, they use two sets of frequencies, foreword and backwards.

Blotto box - This box supposedly shorts every fone out in the immediate area, and I don't doubt it. It should kill every fone in the immediate area, until the voltage reaches the fone company, and the fone company filters it. I won't cover this one in this issue, cuz it is dangerous, and phreaks shouldn't destroy MA's equipment, just phuck it up. Look for this on your phavorite BBS or ask your phavorite phreak for info if you really are serious about seriously phucking some fones in some area.

blue box - An old piece of equipment that emulated a true operator placing calls, and operators get calls for free. The blue box seizes an open trunk by blasting a 2600 Hz tone through the line after dialing a party that is local or in the 800 NPA so calls will be local or free for the blue

boxer. Then, when the blue boxer has seized a trunk, the boxer may then, within the next 10-15 seconds, dial another fone number via MF tones. These MF tones must be preceded by a KP tone and followed with a ST tone. All of these tones are standardized by Bell. The tones as well as the inter-digit intervals are around 75ms. It may vary with the equipment used since ESS can handle

higher speeds and doesn't need inter-digit intervals. There are many uses to a blue box, and we will not cover any more here. See your local phreak or phreak oriented BBS for in depth info concerning blue boxes and blue boxing. Incidentally, blue boxes are not considered safe anymore because ESS detects "foreign" tones, such as the 2600 Hz tone, but this detection may be delayed by mixing pink noise of above 3000 Hz with the 2600 Hz tone. To hang up, the 2600 Hz tone is played again. Also, all blue boxes are green boxes because MF "2" corresponds to the Coin Collect tone on the green box, and the "KP" tone corresponds to the Coin Return tone on the green box. See green box for more information. Blue boxing is IMPOSSIBLE under the new CCIS system slowly being integrated into the Bell system.

blue box tones - The MF tones generated by the blue box in order to place calls, emulating a true operator. These dual tones must be entered during the 10-15 second period after you have seized a trunk with the 2600 Hz tone.

```
                       700:  1 :  2 :  4 :  7 : 11 :    KP= Key
Pulse
parallel Frequencies   900: ** :  3 :  5 :  8 : 12 :    ST= STop
  2= Coin Collect     1100: ** : ** :  6 :  9 : KP :   KP2= Key
Pulse 2
 KP= Coin Return      1300: ** : ** : ** : 10 :KP2 :    **= None
 (green box tones)    1500: ** : ** : ** : ** : ST :
                          : 900:1100:1300:1500:1700:   75ms
pulse/pause
```

BLV - Busy Line Verification. Allows a TSPS operator to process a customer's request for a confirmation of a repeatedly busy line. This service is used in conjunction with emergency break-ins.

BNS - Billed Number Screening. break period - Time when the circuit during pulse dialing is left pen. In the US, this period is 40ms; foreign nations may use 33ms break periods.

break ratio - The interval pulse dialing breaks and makes the loop when dialing. The US standard is 10 pulses per second.

When the circuit is opened, it is called the break interval. When the circuit is closed, it is called the make interval. In the US, there is a 60ms make period and a 40ms break period. This is often referred to as a 60% make interval. Many foreign nations have a 67% make interval.

bridge - I don't really understand this one, but these are important phreak toys. I'll cover them more in the next issue of TPH.

British Post Office - The United Kingdom's equivalent to Ma Bell.

busy box - Box that will cause the fone to be busy, without taking it OFF-HOOK. Just get a piece of fone wire with a plug on the end, cut it off so there is a plug and about two inches of fone line. Then, strip the wire so the two middle wires, the tip and the ring, are exposed. Then, wrap the ring and the tip together, tape with electrical tape, and plug into the fone jack. The fone will be busy until the box is removed.

cans - Cans are those big silver boxes on top of or around the telephone poles. When opened, the lines can be manipulated with a beige box or whatever phun you have in mind.

calling card - Another form of the LD service used by many major LD companies that composes of the customers fone number and a PIN number. The most important thing to know when questioned about calling cards are the area code and the city where the calling card customer originated from.

CAMA - Centralized Automatic Message Accounting. System that records the numbers called by fones and other LD systems. The recording can be used as evidence in court.

CC - Calling Card.

CC - Credit Card.

CCIS - Common Channel Inter-office Signaling. New method being incorporated under Bell that will send all the signaling information over separate data lines. Blue boxing is IMPOSSIBLE under this system.

CCITT - The initials of the name in French of the International Telegraph and Telephone Consultative Committee. At CCITT representatives of telecommunications authorities, operators of public networks and other interested bodies meet to agree on standards needed for international intermarrying of telecommunications services.

CCS - Calling Card Service.

CCSS - Common Channel Signalling System. A system whereby all signalling for a number of voice paths are carried over one common channel, instead of within each individual channel.

CDA - Coin Detection and Announcement.

CF - Coin First. A type of fortress fone that wants your money before you receive a dial tone.

Channel - A means of one-way transmission or a UCA path for electrical transmission between two or more points without common carrier, provided terminal equipment. Also called a circuit, line, link, path, or facility.

cheese box - Another type of box which, when coupled with call forwarding services, will allow one to place free fone calls. The safety of this box is unknown. See references for information concerning text philes on this box.

clear box - Piece of equipment that compromises of a telephone pickup coil and a small amp. This works on the principal that all receivers are also weak transmitters. So, you amplify your signal on PP fortress fones and spare yourself some change.

CN/A - Customer Name And Address. Systems where authorized Bell employees can find out the name and address of any customer in the Bell System. All fone numbers are listed on file, including unlisted numbers. Some CN/A services ask for ID#'s when you make a request. To use, call the CN/A office during normal business hours, and say that you are so and so from a certain business or office, related to customers or something like that, and you need the customer's name and address at (NPA)Nxx-xxxx. That should work. The operators to these services usually know more than DA operators do and are also susceptible to "social engineering." It is possible to bullshit a CN/A operator for the NON PUB DA number and policy changes in the CN/A system.

CO Code - Central Office code which is also the Nxx code. See Nxx for more details. Sometimes known as the local end office.

conference calls - To have multiple lines inter-connected in order to have many people talking in the same conversation on the fone at once. See Alliance and switch crashing for more information.

credit operator - Same as TSPS operator. The operator you get when you dial "0" on your fone and phortress fones. See TSPS for more information.

CSDC - Circuit Switched Digital Capability. Another USDN service that has no ISDN counterpart.

DA - Directory Assistance. See directory assistance.

DAO - Directory Assistance Operator. See directory assistance.

data communications - In telefone company terminology, data communications refers to an end-to-end transmission of any kind of information other than sound, including voice, or video. Data sources may be either digital or analog.

data rate - The rate at which a channel carries data, measured in bits per second, bit/s, also known as "data signalling rate." data signalling rate - Same as "data rate." See data rate.

DCO-CS - Digital Central Office-Carrier Switch.

DDD - Direct Distance Dialed.

Dial-It Services - See 900 Services.

digital - A method to represent information to be discrete or individually distinct signals, such as bits, as opposed to a continuously variable analog signal.

digital transmission - A mode of transmission in which all information to be transmitted is first converted to digital form and then transmitted as a serial stream of pulses. Any signal, voice, data, television, can be converted to digital form.

Dimension 2000 - Another LD service located at (800)848-9000.

directory assistance - Operator that you get when you call 411 or NPA-555-1212. This call will cost $.50 per call. These won't know where you are calling from, unless you annoy them, and do not have access to unlisted numbers. There are also directory assistance operators for the deaf that transfer BAUDOT. You can call these and have interesting conversations. The fone number is 800-855-1155, are free, and use standard Telex abbreviations such as GA for Go Ahead. These are nicer than normal operators, and are often subject to "social engineering" skills (bullshitting). Other operators also have access to their own directory assistance at KP+NPA+131+ST.

diverter - This is a nice phreak tool. What a diverter is is a type of call forwarding system done externally, apart from the fone company, which is a piece of hardware that will foreword the call to somewhere else. These can be found on many 24 hour plumbers, doctors, etc. When you call, you will often hear

a click and then ringing, or a ring, then a click, then another ring, the second ring often sounds different from the first. Then, the other side picks the fone up and you ask about their company or something stupid, but DO NOT ANNOY them. Then eventually, let them hang up, DO NOT HANG UP YOURSELF. Wait for the dial tone, then dial ANI. If the number ANI reads is different from the one you are calling from, then you have a diverter. Call anywhere you want, for all calls will be billed to the diverter. Also, if someone uses a tracer on you, then they trace the diverter and you are safe. Diverters can, however, hang up on you after a period of time; some companies make diverters that can be set to clear the line after a set period of time, or click every once in a while, which is super annoying, but it will still work. Diverters are usually safer than LD extenders, but there are no guarantees. Diverters can also be accessed via phortress fones. Dial the credit operator and ask for the AT&T CREDIT OPERATOR. They will put on some lame recording that is pretty long. Don't say anything and the recording will hang up. LET IT HANG UP, DO NOT HANG UP. Then the line will clear and you will get a dial tone. Place any call you want with the following format: 9+1+NPA+Nxx+xxxx, or for local calls, just 9+Nxx+xxxx. I'd advise that you call ANI first as a local call to make sure you have a diverter.

DLS - Dial Line Service.

DNR - Also known as pen register. See pen register.

DOV - Data-Over-Voice.

DSI - Data Subscriber Interface. Unit in the LADT system that will concentrate data from 123 subscribers to a 56k or a 9.6k bit-per-second trunk to a packet network.

DT - Dial tone.

DTF - Dial Tone First. This is a type of fortress fone that gives you a dial tone first.

DTI - Digital Trunk Interface.

DTMF - Dual-Tone-Multi-Frequency, the generic term for the touch tone. These include 0,1,2,3,4,5,6,7,8,9 as well as A,B,C,D. See silver box for more details.

DVM - Data Voice Multiplexor. A system that squeezes more out of a transmission medium and allows a customer to transmit voice and data simultaneously to more than one receiver over the existing telefone line.

emergency break-in - Name given to the art of "breaking" into a busy number which will usually result in becoming a third party in the call taking place.

end office - Any class 5 switching office in North America.

end-to-end signalling - A mode of network operation in which the originating central office, or station, retains control and signals directly to each successive central office, or PBX, as trunks are added to the connection.

ESS - Electronic Switching System. "The phreak's nightmare come

true." With ESS, EVERY SINGLE digit you dial is recorded, even mistakes. The system records who you call, when you call, how long you talked, and, in some cases, what you talked about. ESS is programed to make a list of people who make excessive 800 calls or directory assistance. This is called the "800 Exceptional Calling Report." ESS can be programed to print out logs of who called certain numbers, such as a bookie, a known communist, a BBS, etc. ESS is a series of programs working together; these programs can be very easily changed to do whatever the fone company wants ESS to do. With ESS, tracing is done in MILLISECONDS and will pick up any "foreign" tones on the line, such as 2600 Hz. Bell predicts the whole country will be on ESS by 1990! You can identify an ESS office by the functions, such as dialing 911 for help, fortress fones with DT first, special services such as call forwarding, speed dialing, call waiting, etc., and ANI on LD calls. Also, black boxes and Infinity transmitters will NOT work under ESS.

extender - A fone line that serves as a middleman for a fone call, such as the 800 or 950 extenders. These systems usually require a multi- digit code and have some sort of ANI to trace suspicious calls with.

facsimile - A system for the transmission of images. The image is scanned at the transmitter, reconstructed at the receiving station, and duplicated on some form of paper. Also known as a FAX.

FAX - See facsimile for details.

FiRM - A large cracking group who is slowly taking the place of PTL and the endangered cracking groups at the time of this writing.

fortress phone - Today's modern, armor plated, pay fone. These may be the older, 3 coin/coin first fones or the newer, 1 coin/DT first fones. There are also others, see CF, DTF, and PP. Most phortresses can be found in the 9xxx or 98xx series of your local Nxx.

gateway city - See ISC.

Gestapo - The telefone company's security force. These nasties are the ones that stake out misused phortresses as well as go after those bad phreaks that might be phucking with the fone system.

green base - A type of output device used by the fone company. Usually light green in color and stick up a few feet from the ground. See output device for more information.

green box - Equipment that will emulate the Coin Collect, Coin Return, and Ringback tones. This means that if you call someone with a fortress fone and they have a green box, by activating it, your money will be returned. The tones are, in hertz, Coin Collect=700+1100, Coin Return=1100+1700, and Ringback=700+1700. However, before these tones are sent, the MF detectors at the CO must be alerted, this can be done by sending a 900+1500 Hz or single 2600 Hz wink of 90ms followed by a 60ms gap, and then the appropriate signal for at least 900ms.

gold box - This box will trace calls, tell if the call is being traced, and can change a trace.

grey box - Also known as a silver box. See silver box.

group chief - The name of the highest ranking official in any fone office. Ask to speak to these if an operator is giving you

trouble. high-speed data - A rate of data transfer ranging upward from 10,000 bits per second.

H/M - Hotel/Motel.

ICH - International Call Handling. Used for overseas calls.

ICVT - InComing Verification Trunk.

IDA - Integrated Digital Access. The United Kingdom's equivalent of ISDN.

IDDD - International Direct Distance Dialing - The ability to place international calls direct without processing through a station. Usually, one would have to place the call through a 011, station, or a 01, operator assisted, type of setup.

IDN - Integrated Digital Networks. Networks which provide digital access and transmission, in both circuit switched and packet modes.

in-band - The method of sending signaling information along with the conversion using tones to represent digits.

INS - Information Network System. Japan's equivalent of ISDN.

Intercept - The intercept operator is the one you get connected to when there are not enough recordings available to tell you that the number has been disconnected or changed. These usually ask what number you are calling and are the lowest form of the operator.

intermediate point - Any class 4X switching office in North America. Also known as an RSU.

international dialing - In order to call across country borders, one must use the format PREFIX + COUNTRY CODE + NATION #. The prefix in North America is usually 011 for station-to-station calls or 01 for operator-assisted calls. If you have IDDD, you don't need to place this prefix in.

INTT - Incoming No Test Trunks.

INWARD - An operator that assists your local TSPS '0' operator in connecting calls. These won't question you as long as the call is within their service area. The operator can ONLY be reached by other operators or a blue box. The blue box number is KP+NPA+121+ST for the INWARD operator that will help you connect to any calls in that area ONLY.

INWATS - Inward Wide Area Telecommunications Service. These are the 800 numbers we are all familiar with. These are set up in bands; 6 total. Band 6 is the largest, and you can call band 6 INWATS from anywhere in the US except the state where the call is terminated. This is also why some companies have a separate 800 number for their state. Band 5 includes the 48 contiguous states. All the way down to band 1, which only includes the states contiguous to that one. Understand? That means more people can reach a band 6 INWATS as compared to the people that can access a band 1 INWATS.

IOCC - International Overseas Completion Centre. A system which must be dialed in order to re-route fone calls to countries

inaccessible via dialing direct. To route a call via IOCC with a blue box, pad the country code to the RIGHT with zeroes until it is 3 digits. Then KP+160 is dialed, plus the padded country code, plus ST.

IPM - Interruptions Per Minute. The number of times a certain tone sounds during a minute.

ISC - Inter-Nation Switching Centers. Most outgoing calls from a certain numbering system will be routed through these gateway cities" in order to reach a foreign country.

SDN - Integrated Services Digital Network. ISDN is a lanned hierarchy of digital switching and transmission ystems. Synchronized so that all digital elements speak the same language" at the same speed, the ISDN would provide voice, data, nd video in a unified manner.

TT - This is another large LD service. The extenders owned by his company are usually considered dangerous. The format is CC-ESS#,(NPA)Nxx-xxxx,1234567.

kpk - Key Pulse. Tone that must be generated before inputting a one number using a blue box. This tone is, in hertz, 1100+1700.

P2 - Key Pulse 2. Tone that is used by the CCITT SYSTEM 5 for pecial international calling. This tone is, in hertz, 1300+1700.

ADT - Local Area Data Transport. LADT is a method by which ustomers will send and receive digital data over existing customer oop wiring. Dial-Up LADT will let customers use their lines or occasional data services; direct access LADT will transmit imultaneous voice and data traffic on the same line.

LAN - Local Area Network.

LAPB - Link Access Protocol Balanced.

LD - Long Distance

leave Word And Call Back - Another new type of operator.

local loop - When a loop is connected between you and your CO. his occurs when you pick the fone up or have a fone OFF-HOOK.

Loop - A pair or group of fone lines. When people call these lines, they can talk to each other. Loops consist of two or more numbers, they usually are grouped close together somewhere in the Nxx-99xx portions of your exchange. The lower number in a loop is the tone side of the loop, or the singing switch. The higher number is always silent. The tone disappears on the lower # when someone dials the other side of the loop. If you are the higher #, you will have to listen to the clicks to see if someone dialed into the loop. There also are such things as Non-Supervised loops, where the call is toll-free to the caller. Most loops will be muted or have annoying clicks at connection, but otherwise, you might find these useful

goodies scanning the 99xx's in your exchange. Some loops allow multi-user capability; thus, many people can talk to each other at the same time, a conference of sorts. Since loops are genuine

test functions for the telco during the day, most phreaks scan and use them at night.

MA - Ma Bell, the Bell Telesys Company. Telco, etc. See Ma Bell for more information.

Ma Bell - The telephone company. The Bell Telesys Phone Company. The company you phreak and hack with. The company that doesn't like you too much. The company you often phuck with, and sometimes phuck up. The company that can phuck u up if u aren't careful.

make period - The time when, during pulse dialing, the circuit is closed. In the US, this period is 60ms; however, foreign nations may use a 67ms make period. Make periods are also referred to in percentages, so a 60ms make period would be 60%, a 67ms as 67%.

marine verify - Another type of operator.

MCI - Yet another LD service that owns many dial-ups in most areas. However, the codes from various areas may not be interchangeable. Not much is known about MCI; however, MCI probably has some sophisticated anti-phreak equipment. The format is ACC-ESS#,12345,(NPA)Nxx-xxxx.

MCI Execunet - The calling card equivalent of the regular MCI LD service, but the codes are longer and interchangeable. For the local access port near you, call (800)555-1212. The format for the port will be ACC-ESS#,1234567,(NPA)Nxx-xxxx.

Metrofone - Owned by Western Union. A very popular system among fone phreaks. Call Metrofone's operator and ask for the local access number at (800)325-1403. The format is ACC-ESS#,CODE,(NPA)Nxx-xxxx. Metrofone is alleged to place trap codes on phreak BBS's.

MF - Multi-Frequency. These are the operator and blue box tones. An MF tone consists of two tones from a set of six master tones which are combined to produce 12 separate tones. These are NOT the same as touch tones. See blue box tones for frequencies.

mobile - A type of operator.

NAP/PA - North American Pirate/Phreak Association. A large group of bbs boards which include a lot of pirates/phreakers. I'm not quite sure where the group will go from here.

NON PUB DA - A reverse type of CN/A bureau. You tell the service the name and the locality, they will supply the fone number. However, they will ask for you name, supervisor's name, etc. Use your social engineering skills here (aka, bullshitting skills). You also can get detailed billing information from these bureaus.

NPA - Numbering Plan Area. The area code of a certain city/state. For example, on the number (111)222-3333, the NPA would be 111. Area codes never cross state boundaries sans the 800, 700, 900, and special exchanges.

Nxx - The exchange or prefix of the area to be dialed. For example of the number (111)222-3333, the Nxx would be 222.

OGVT - OutGoing Verification Trunk.

OFF-HOOK - To be on-line, to have the switchhook down. To have a

closed connection. At this point, you also have a local loop.

ON-HOOK - To be off-line, to have the switchhook up. To have an open connection.

ONI - Operator Number Identification. Identifies calling numbers when an office is not equipped with CAMA, the calling number is not automatically recorded by CAMA, or has equipment failures, such as ANIF.

OPCR - Operator Actions Program. Standard TBOC or equivalent "0" operator.

OPEN - Northern Telecom's Open Protocol Enhanced Networks World Program.

OSI - Open System Interconnection. Form of telecommunication architechture which will probobly fail to SNA.

OST - Originating Station Treatment.

OTC - Operating Telefone Company.

out-of-band - Type of signaling which sends all of the signaling and supervisory informations, such as ON and OFF HOOK, over separate data links.

output device - Any type of interface such as cans, terminal sets, remote switching centers, bridging heads, etc., where the fone lines of the immediate area are relayed to before going to the fone company. These often are those cases painted light green and stand up from the ground. Most of these can be opened with a 7/16 hex driver, turning the security bolt(s) 1/8 of an inch counter-clockwise, and opening. Terminals on

the inside might be labeled "T" for tip and "R" for ring. Otherwise, the ring side is usually on the right and the tip side is on the left.

OUTWATS - Outward Wide Area Telecommunications Service. These are WATS that are used to make outgoing calls ONLY.

Paper Clip Method - This method of phreaking was illustrated in the movie War Games. What a phortress fone does to make sure money is in a fone is send an electrical pulse to notify the fone that a coin has been deposited, for the first coin only. However, by simply grounding the positive end of the microphone, enough current and voltage is deferred to the ground to simulate the first quarter in the coin box. An easy way to accomplish this is to connect the center of the mouthpiece to the coin box, touch tone pad, or anything that looks like metal with a piece of wire. A most convenient piece of wire is a bend out of a paper clip. Then you can send red box tones through the line and get free fone calls! Also, telco modified fones may require you to push the clip harder against the mouthpiece, or connect the mouthpiece to the earpiece. If pressing harder against the mouthpiece becomes a problem, pins may be an easier solution.

PBX - Private Branch eXchange. A private switchboard used by some big companies that allow access to the OUTWATS line by dialing a 8 or a 9 after inputting a code.

PCM - Pulse Code-Modulated trunks.

PC Pursuit - A computer oriented LD system, comparable to Telenet, which offers low access rates to 2400 baud users. Hacking

on this system is virtually impossible due to the new password format.

pen register - A device that the fone company puts on your line if they suspect you are fraudulently using your fone. This will record EVERY SINGLE digit/rotary pulse you enter into the fone as well as other pertinent information, which may include a bit of tapping. Also known as DNR.

Phortune 500 - An elite group of users currently paving the way for better quality in their trade.

PHRACK - Another phreak/hack oriented newsletter. See reference section, phile 1.6 for more information.

PHUN - Phreakers and Hackers Underground Network. They also release a newsletter that is up to #4 at the time of this writing. See phile 1.6 for more information on finding this phile.

PIN - Personal Identification Number - The last four digits on a calling card that adds to the security of calling cards.

plant tests - test numbers which include ANI, ringback, touch tone tests, and other tests the telco uses.

Post Office Engineers - The United Kingdom's fone workers.

PP - Dial Post-Pay Service. On phortress fones, you are prompted to pay for the call after the called party answers. You can use a clear box to get around this.

PPS - Pulses Per Second.

printmeter - The United Kingdom's equivalent of a pen register. See pen register for more info.

PTE - Packet Transport Equipment.

PTL - One of the bigger cracking groups of all time. However, the group has been dying off and only has a few nodes as of this writing.

PTS - Position and Trunk Scanner.

PTT - Postal Telephone Telegraph.

pulse - See rotary phones.

purple box - This one would be nice. Free calls to anywhere via blue boxing, become an operator via blue box, conference calling, disconnect fone line(s), tap fones, detect traces, intercept directory assistance calls. Has all red box tones. This one may not be available under ESS.

rainbow box - An ultimate box. You can become an operator. You get free calls, blue box. You can set up conference calls. You can forcefully disconnect lines. You can tap lines. You can detect traces, change traces, and trace as well. All incoming calls are free. You can intercept directory assistance. You have a generator for all MF tones. You can mute and redial. You have all the red-box tones. This is an awesome box. However, it does not exist under ESS.

RAO - Revenue Accounting Office. The three digit code that sometimes replaces the NPA of some calling cards.

RBOC - Regional Bell Operating Company.

red box - Equipment that will emulate the red box tone generated for coin recognition in all phortress fones.

red box tones - Tones that tell the phortress fone how much money was inserted in the fone to make the required call. In one slot fones, these are beeps in pulses; the pulse is a 2200+1700 Hz tone. For quarters, 5 beep tones at 12-17 PPS, for dimes it is 2 beep tones at 5-8.5 PPS, and a nickel causes 1 beep tone at 5-8.5 PPS. For three slot fones, the tones are different. Instead of beeps, they are straight dual tones. For a nickel, it is one bell at 1050-1100 Hz, two bells for a dime, and one gong at 800 Hz for a quarter. When using red box tones, you must insert at least one nickel before playing the tones, cuz a ground test takes place to make sure some money has been inserted. The ground test may be fooled by the Paper Clip Method. Also, it has been known that TSPS can detect certain red box tones, and will record all data on AMA or CAMA of fraudulent activity.

regional center - Any class 1 switching office in North America.

REMOB - Method of tapping into lines by entering a code and the 7 digit number you want to monitor, from ACD Test Mode. A possibility of this may be mass conferencing.

ring - The red wire found in fone jacks and most fone equipment. The ring also is less positive than the tip. When looking at a fone plug on the end of typical 4 wire fone line from the top, let's say the top is the side with the hook, the ring will be the middle-right wire. Remember, the ring is red, and to the right. The three "R's" revived!

ring-around-the-rosy - 9 connections in tandem which would cause an endless loop connection and has never occurred in fone history.

ringback - A testing number that the fone company uses to have your fone ring back after you hang up. You usually input the three digit ringback number and then the last four digits to the fone number you are calling from.

ring trip - The CO process involved with stopping the AC ringing signal when a fone goes OFF-HOOK.

rotary phone - The dial or pulse phone that works by hooking and un-hooking the fone rapidly in secession that is directly related to the number you dialed. These will not work if another phone with the same number is off-hook at the time of dialing.

Rout & Rate - Yet another type of operator; assists your TSPS operator with rates and routings. This once can be reached at KP+800+141+1212+ST.

RPE - Remote Peripheral Equipment.

RQS - The Rate Quote System. This is the TSPS operator's rate/quote system. This is a method your '0' operator gets info without dialing the rate and route operator. The number is KP+009+ST.

RSU - Remote Switching Unit. The class 4X office that can

have an unattended exchange attached to it.

RTA - Remote Trunk Arrangement.

SAC - Special Area Code. Separate listing of area codes, usually for special services such as TWX's, WATS, or DIAL-IT services.

SCC - Specialized Common Carriers. Common Nxx numbers that are specialized for a certain purpose. An example is the 950 exchange. sectional center - Any class 2 switching office in North America. service monitoring - This is the technical name of phone tapping.

SF - Supervision Control Frequency. The 2600 Hz tone which seizes any open trunk, which can be blue boxed off of.

short-haul - Also known as a local call.

signalling - The process by which a caller or equipment on the transmitting end of a line in: forms a particular party or equipment at the receiving end that a message is to be communicated. Signalling is also the supervisory information which lets the caller know the called know the called party is ready to talk, the line is busy, or the called party has hung up.

silver box - Equipment that will allow you to emulate the DTMF tones A,B,C,D. The MF tones are, in hertz, A=697+1633, B=770+1633, C=852+1633, D=941+1633. These allow special functions from regular fones, such as ACD Testing Mode.

Skyline - Service owned by IBM, Comsat, and AEtna. It has a local access number in the 950 exchange. The fone number is 950-1088. The code is either a 6 or 8 digit number. This company is alleged to be VERY dangerous.

SNA - System Network Architechture, by IBM. A possible future standard of architechture only competed by OSI.

SOST - Special Operator Service Treatment. These include calls which must be transferred to a SOST switchboard before they can be processed; services such as conferences, appointments, mobile, etc.

SPC - Stored Program Control. Form of switching the US has heavily invested in.

Sprint - One of the first LD services, also known as SPC. Sprint owns many extender services and is not considered safe. It is common knowledge that Sprint has declared war on fone phreakers.

SSAS - Station Signaling and Announcement System. System on most fortress fones that will prompt caller for money after the number, usually LD numbers, has been dialed, or the balance due before the call will be allowed to connect.

stacking tandems - The art of busying out all trunks between two points. This one is very amusing.

STart - Pulse that is transmitted after the KP+NPA+Nxx+xxxx through operator or blue boxed calls. This pulse is, in hertz, 1500+1700.

station # - The last four digits in any seven digit fone number.

STD - Subscriber Trunk Dialing. Mechanism in the United Kingdom which takes a call from the local lines and legimately elevates it to a trunk or international level.

step crashing - Method of using a rotary fone to break into a busy line. Example, you use a rotary fone to dial Nxx-xxx8 and you get a busy signal. Hang up and dial Nxx-xxx7 and in between the last pulse of your rotary dial and before the fone would begin to ring, you can flash your switchhook extremely fast. If you do it right, you will hear an enormous "CLICK" and all of a sudden, you will cut into your party's conversation.

STPS - Signal Transfer PointS. Associated with various switching machines and the new CCIS system.

switchhook - The button on your fone that, when depressed, hangs the fone up. These can be used to emulate rotary dial fones if used correctly.

SxS - Step-By-Step. Also known as the Strowger Switch or the two-motion switch. This is the switching equipment Bell began using in 1918. However, because of its limitations, such as no direct use of DTMF and maintenance problems, the fone company has been upgrading since. You can identify SxS switching offices by lack of DTMF or pulsing digits after dialing DTMF, if you go near the CO it will sound like a typewriter testing factory, lack of speed calling, lack of special services like call forwarding and call waiting, and fortress fones want your money first, before the dial tone.

TAP - The "official" phone phreak's newsletter. Previously YIPL.

T&C - Time and Charge.

tapping - To listen in to a phone call taking place. The fone company calls this "service monitoring."

TASI - Time Assignment Speech Interpolation. This is used on satellite trunks, and basically allows more than one person to use a trunk by putting them on while the other person isn't talking.

Telenet - A computer-oriented system of relay stations which relay computer calls to LD numbers. Telenet has a vast array of access ports accessible at certain baud rates.

Tel-Tec - Another LD company that usually give out a weak connection. The format is (800)323-3026,123456,(NPA)Nxx-xxxx.

Tel-Tex - A subsidiary of Tel-Tec, but is only used in Texas. The number is *800)432-2071 and the format is the same as above.

terminal - A point where information may enter or leave a communication network. Also, any device that is capable of sending and/or receiving data over a communication channel.

tip - The green wire found in fone jacks and most fone equipment. The tip is the more positive wire compared to the ring. When looking at a fone plug from the top, lets say the hook side is the top, the tip will be the middle wire on the left.

toll center - Any class 4 switching office located in North America.

toll point - Any class 4P switching office in North America.

Toll LIB - Reverse CN/A bureau. See NON PUB DA for more info.

touch tone phone - A phone that uses the DTMF system to place calls.

touch tone test - This is another test number the fone company uses. You dial the ringback number and have the fone ring back. Then, when you pick it up, you will hear a tone. Press your touch-tone digits 1-0. If they are correct, the fone will beep twice.

trace - Something you don't want any fone company to do to you. This is when the fone company you are phucking with flips a

switch and they find the number you are calling from. Sometimes the fone company will use ANI or trap and trace methods to locate you. Then the local Gestapo home in and terminate the caller if discovered.

trap and trace - A method used by the FBI and some step offices that forces a voltage through the line and traces simultaneously, which mean that you can't hang up unless the Pheds do, and pray you aren't calling from your own house. Trap and trace is also known as the lock-in-trace.

trap codes - Working codes owned by the LD company, not a customer, that, when used, will send a "trouble card" to Ma Bell, no matter what company the card is coming from, and ESS will immediately trace the call. Trap codes have been in use for some time now, and it is considered safer to self-hack codes opposed to leeching them off of BBS's, since some LD companies post these codes on phreak oriented BBS's.

Travelnet - Service owned by GM that uses WATS as well as local access numbers. Travelnet also accepts voice validation for its LD codes.

TSPS - Traffic Service Position System. Operator that usually is the one that obtains billing information for Calling Card or 3rd number calls, identifies called customer on person-to-person calls, obtains acceptance of charges on collect calls, or identifies calling numbers. These operators have an ANI board and are the most dangerous type of operator.

TWX - Telex II consisting of 5 teletypewriter area codes. These are owned by Western Union. These may be reached via another TWX machine running at 110 baud. You can send TWX messages via Easylink (800)325-4122.

USDN - United States Digital Network. The US's version of the ISDN network.

videotext - Generic term for a class of two-way, interactive data distribution systems with output typically handled as in teletext systems and input typically accepted through the telephone or public data network.

WATS - Wide Area Telecommunications Service. These can be IN or OUT, see the appropriate sections.

WATS Extender - These are the LD companies everyone hacks and phreaks off of in the 800 NPA. Remember, INWATS + OUTWATS = WATS Extender.

white box - This is a portable DTMF keypad.

XBAR - Crossbar. Crossbar is another type of switching equipment the fone company uses in some areas. There are three major types of Crossbar systems called No.1 Crossbar (1XB), No.4 Crossbar (4XB), and No.5 Crossbar (5XB). 5XB has been the primary end office switch of MA since the 60's and
is still in wide use. There is also Crossbar Tandem (XBT) used for toll-switching.

XBT - Crossbar Tandem. Used for toll-switching. See XBAR.

YIPL - The classic "official" phreak's magazine. Now TAP.

Other Fone Information

Voltages & Technical Stuff

When your telephone is ON-HOOK, there is 48 volts of DC across the tip and the ring. When the handset of a fone is lifted a few switches close which cause a loop to become connected between you and the fone company, or OFF-HOOK. This is also known as the local loop. Once this happens, the DC current is able to flow through your fone with less resistance. This causes a relay to energize which causes other CO equipment to realize that you want service. Eventually, you will end up with a dial tone. This also causes the 48 VDC to drop down to around 12 VDC. The resistance of the loop also drops below the 2500 ohm level; FCC licensed telephone equipment must have an OFF-HOOK impedance of 600 ohms.

When your fone rings, the telco sends 90 volts of pulsing AC down the line at around 15-60 Hz, usually 20 Hz. In most cases, this causes a metal armature to be attracted alternately between two electromagnets; thus, the armature often ends up striking two bells of some sort, the ring you often hear when non-electronic fones receive a call. Today, these mechanical ringers can be replaced with more modern electronic bells and other annoying signaling devices, which also explains why deaf people can have lights and other equipment attached to their fones instead of ringers.

When you dial on a fone, there are two common types of dialing, pulse and DTMF. If you are like me, you probably don't like either and thought about using MF or blue box tones. Dialing rotary breaks and makes connections in the fone loop, and the telco uses this to signal to their equipment that you are placing a call. Since it is one fone that is disconnecting and reconnecting the fone line, if someone else picks up another fone on the same extension, both cannot make pulse fone calls until one hangs up. DTMF, on the other hand, is a more modern piece of equipment and relies on tones generated by a keypad, which can be characterized by a 0,1,2,3,4,5,6,7,8,9/A,B,C,D keypad. Most fones don't have

an A,B,C,D keypad, for these frequencies are used by the telco for test and other purposes.

Scanning Phun Fone Stuff

Scanning is the act of either randomly or sequentially dialing fone numbers in a certain exchange when you are looking for several different things. These things could be carriers, extenders, ANI, "bug tracers," loops, as well as many other interesting "goodies" the fone company uses for test purposes.

When scanning for carriers, your local BBS probably has some scanning programs, as these became popular after the movie

WARGAMES, but what these do are to call every fone in an exchange, or a specified range of fone numbers in certain exchanges to look for possible carriers and other interesting computer equipment. So, if your computer finds a carrier, or what seems like a carrier, it will either print it out or save it in some file for later reference. With these carriers one finds, one can either call them and find out what each is or, if one of them is interesting, one can hack or attempt to break into some interesting systems available, not to the general public, of course.

Scanning telephone "goodies" requires time and patience. These goodies usually cannot be traced by most unmodified modems, as the frequencies and voice transmissions cannot be differentiated from other disturbances, such as the annoying operator saying, "We're sorry... blah blah..". Anyway, to scan these, you usually get a regular carrier scanner and, with the modem speaker on, sit by your wonderful computer and listen in on the scanning for any interesting tones, voices, or silences, which could be telco fone phun numbers, for us of course! Then write these down, and spread them around, use, abuze, etc. if you dare. Anyway, most telefone goodies are located in the 99xx suffixes of any fone exchange. If you found everything you think in the exchanges you have scanned, try the 0xxx and 1xxx suffixes in that order. You might even find loops, ANI, and other phun things if you mess around enough.

References & Suggested Reading

The following is a list of references and suggested reading for the beginning, as well as advanced phreak. See you local fone phreak for these, or call your local phreak oriented BBS for information regarding these publications.

2600 Magazine

Aqua Box, The By Captain Xerox & The Traveler

Basic Alliance Teleconferencing By The Trooper

Bell Hell By The Dutchman & The Neon Knights

Better Homes And Blue Boxing By Mark Tabas

BIOC Agent 003's Course In Basic Telecommunications
By BIOC Agent 003

History Of British Phreaking, By Lex Luthor & The Legion Of Doom

Home Phone Tips By 13th Floor Enterprises

How To Build A Blotto Box By The Traveler

How To Build A Cheese Box By Mother Phucker

Introducing The Beige Box - Construction & Use
By The Exterminator and The Terminal Man

Integrated Services Digital Network [ISDN]
By Zander Zan

LOD/H Technical Journal

Loops I've Known And Loved By Phred Phreak

PHRACK Magazine

950's: The Real Story: by Jester

Ever heard (actually, seen) people on various hacking boards around the country telling you how you are going to get caught for sure if you use the in state-WATS (950) telephone numbers to make your phreaks off of? This file is to tell you what the story is with 950's and how to SAFELY use them. The 950 prefix was created by the old Bell System for all the SSC's (Specialized Common Carrier), or Extenders as they are called, to place their services upon. This was done for the long distance company's benefit so they could have the same dialup in all cities across the USA. For some reason, the Long Distance companies rejected the 950 prefix in favor of local lines and 1-800 numbers.

Disadvantages to 950's are that they are run on a special ESS of their own that can trace you call before you can say 'shit!'. But tracing only occurs on special occasions. The companies on 950's will only trace when the computer controlling the calls sees that there is an unusually high number of calls to the extender on that particular day. The computer then will auto-trace every 100th call or so. Which means that, if used in moderation, 950's are fantastic!

Advantages: By having the same dialup in all cities, you can go on vacation and just hack codez to use for while you are there on your favorite 950 extender. Being a free call (in most cases, some phones not) from a pay phone, this is very advantageous. Also, and anyone who has used a 950 knows this, the connections on 950 extenders are VERY clear usually, making for excellent error-free data transfer on AE lines, etc.

With the breakup of the Bell System in January of 1984, the 950 prefix was supposed to be dragged down with it and the companies were supposed to have switched over to either local or 1-800 numbers, but as is very typical of the phone company, they never got around to it.

Here is the list of the 950's that are currently in use in the U.S. :

950-1000.....Southern Pacific Communications
950-1022.....MCI Exec-U-Net
950-1033.....U.S. Telephone

950-1044.....AllNet
950-1066.....Lexitel
950-1088.....SBS Skyline

Personally, I favor the use of 950-1088, because it has many users and the codez (which, by the way are 6 digits, but they are switching over to 8 igits) are easy to hack out from a pay phone. You may want to try the other services so you can have a few codez from each available for use.

Automatic Number Identifier: By Jester

Automatic Number Identification

Automatic Number Identification (ANI) is nothing more than automatic means for immediately identifying the Directory Number of a calling subscriber. This process made it possible to utilize CAMA* (Centralized Automatic Message Accounting) systems in SxS, Panel, and Xbar #1 offices. The identity of the calling line is determined by ANI circuits installed in the types of CO's mentioned above. Xbar#5 offices have their own AMA (Automatic Message Accounting) equipment and utilize an AMA translator for automatically identifying the calling line.

Before ANI was developed, each subscriber line (also called a local loop) had a mechanical marking device that kept track of toll charges. These devices were manually photographed at the end of the billing period and the amount of the subscribers bill was determined from that. This process was time consuming, so a new system (ANI) was developed.

The major components of the ANI system used in SxS and Crossbar #1 are: Directory number network and bus arrangement* for connecting the sleeve (the lead that is added to the R(ing) and T(ip) wires of a cable pair at the MDF* (Main Distribution Frame)); A lead of each line number through an identifier connector to the identifier circuit; Outpulser and Identifier connector circuit to seize an idle Identifier; Identifier circuit to ascertain the calling party's number and send it to the outpulser for subsequent transmission through the outpulser link to the ANI outgoing trunk; An ANI outgoing trunk to a Tandem office equipped with a CAMA system.

The following is a synopsis of the ANI operations with respect to a toll call through a #1Xbar office. The call is handled in the normal manner by the CO equipment and is routed through an ANI outgoing trunk to a Tandem office. The identification process starts as soon as all digits of the called number are received by the CAMA sender in the Tandem office and when the district juncture in the Xbar office advances to its cut-through position (a position of the connecting circuits or paths between the line-link and trunk-link frames in the CO).

Upon receiving the start identification signal from the CAMA equipment, the ANI outgoing trunk (OGT) establishes a connection through an outpulser link to an idle outpulser circuit. An idle identifier is then seized by the outpulser circuit through an internal Identifier connector unit. Then the identifier through the connector unit connects to the directory number network and bus system.

At the same time, the identifier will signal the ANI trunk to apply a 5800Hz identification tone to the sleeve lead of the ANI trunk. The tone is transmitted at a two-volt level over the S lead paths through the directory number network and bus system. It will be attenuated or decreased to the microvolt range by the time the identifier circuit is reached, necessitating a 120dB voltage amplification by the amplifier detector equipment in the identifier to insure proper digit identification and registration operations.

A single ANI installation can serve as many as six CO's in a multi-office building. The identifier starts its search for the calling line number by testing or scanning successively the thousands secondary buses of each CO. When the 5800Hz signal is detected, the identifier grounds corresponding leads to the outpulser, to first register the digit of the calling office and then the thousands digit of the calling subscriber's number. The outpulser immediately translates the digit representing the calling office code into its own corresponding three digit office code. The identifier continues its scanning process successively on the groups of hundreds, tens, and units secondary buses in the calling office, and the identified digits of the calling number are also registered and translated in the outpulser's relay equipment for transmission to the tandem office. The outpulser is equipped with checking and timing features to promptly detect and record troubles encountered (This process may be responsible for some of the cards found while trashing). Upon completion of the scanning process, it releases the identifier and proceeds to outpulse in MF tones the complete calling subscriber's number to the CAMA equipment in the tandem office in the format of KP+X+PRE+SUFF+ST where the X is an information digit. The information digits are as follows:
0-Automatic Identification (normal)
1-Operator Identification (ONI)*
2-Identification Failure (ANIF)*

(There is also other types of outpulsing of ANI information if the calling line has some sort of restriction on it).

When all digits have been transmitted and the ANI trunk is cut-through for talking, the outpulser releases.

In the tandem office, the calling party's number is recorded on tape in the CAMA equipment together with other data required for billing purposes. This information, including the time of when the called station answered and the time of disconnect, goes on AMA tapes. The tapes themselves are usually standard reel to reel magnetic tape, and are sent to the Revenue Accounting Office or RAO at the end of the billing period.

So, to sum the entire ANI process up:

The toll call is made. The CO routes the call through ANI trunks where an idle identifier is seized which then connects to the directory number network and bus system while signalling the ANI trunk to apply the needed 5800Hz tone to the Sleeve. The identifier begins a scanning process and determines the calling office number and the digits of the calling subscriber's number, which is sent by way of the outpulser in MF tones to the CAMA equipment in the tandem office. The call information is recorded onto AMA tapes and used to determine billing.

Note that your number does show up on the AMA tape, if the circumstances are correct, (any toll call, whether it is from a message-rate line or from a flat-rate line). However, the AMA tapes

do not record the calling line number in any separated format. They are recorded on a first-come, first-serve basis.

Misc. Footnotes (denoted by an asterisk in the main article)
---

* ANIF-Automatic Number Identification Failure. This is when the ANI equipment does not work properly, and could occur due to a wide variety of technicalities. When ANIF occurs, something called ONI (Operator Number Identification) is used. The call is forwarded to a TSPS operator who requests the calling line number by saying something similar to 'What number are you calling from?'

* CAMA-Centralized Automatic Message Accounting. CAMA is a system that records call details for billing purposes. CAMA is used from a centralized location, usually a Tandem office. CAMA is usually used to serve class 5 End Offices in a rural area near a large city which contains a Tandem or Toll Office. CAMA is similar to LAMA, except LAMA is localized in a specific CO and CAMA is not.

* The Directory Number Network and bus system is a network involved with the ANI process. It is a grid of vertical and horizontal buses, grouped and classified as Primary or Secondary. There are 100 vertical and 100 horizontal buses in the Primary system. In the Secondary system, there are two sub-groups: Bus system #1 and Bus system #2, both of which have ten horizontal and vertical buses. These buses as a whole are linked to the Identifier in the ANI trunk and are responsible for identifying tens, hundreds, thousands and units digits of the calling number (After the Identifier begins its scanning process).

* MDF-Main Distribution Frame. This is the area where all cable pairs of a certain office meet, and a third wire, the Sleeve wire, is added. The Sleeve wire is what is used in gathering ANI

information, as well as determining a called lines status (off/on hook) in certain switching systems by presence of voltage. (voltage present on Sleeve, line is busy, no voltage, line is idle.)

* ONI-Operator Number Identification. See ANIF footnote.

NOTE: There are also other forms of Automatic Message Accounting, such as LAMA (Local Automatic Message Accounting). LAMA is used in the class 5 End Office as opposed to CAMA in a Toll Office. If your End Office had LAMA, then the ANI information would be recorded at the local level and sent from there. The LAMA arrangement may be computerized, in which it would denoted with a C included (LAMA-C or C-LAMA).